Contents

CYBER SECURITY

UNIT 1

INTRODUCTION TO CYBERCRIME, CHALLENGES OF CYBERCRIME, CLASSIFICATION OF CYBERCRIMES – E-MAIL SPOOFING, SPAMMING, INTERNET TIME THEFT, SALAMI ATTACK/SALAMI TECHNIQUE

Q.1. Give the definition of cybercrime.

Ans. Giving an opinion for defining cybercrime is very difficult. The definition which was initially given for cybercrime is –

"A crime conducted in which a computer was directly and significantly instrumental."

Since this definition was not accepted by all, but it give a narrow scope for defining "cybercrime".

Another definition given for cybercrime is as follow –

"Any illegal behaviour that targets the security of computer systems and the data processed by them, which is directed by any electronic operation, is called cybercrime".

The term cybercrime besides the "computer crime" has other names also such as "Internet crime, E-crime, High-tech crime, computer-related crime etc." Computer crime can be defined in number of ways some of them are as follows –

(i) A special knowledge of computer technology is essential for investigation and prosecution of any illegal act, then this illegal act is known as cybercrime.

(ii) Using computational environment making any financial fraud with banks/customers etc.

(iii) Steal a person's identity, by using a computer and Internet, is also a computer crime.

Q.2. What are the challenges of cybercrime ? Explain.

Or

What are the various challenges of cybercrime ? (R.G.P.V., Nov. 2019)

Ans. There are many drawbacks of cybercrime in India. Cybercrime is prevented from being addressed in India, just because of these drawbacks. Most of the Indians do not report the cybercrimes to law enforcement agencies and besides this many peoples in our country are not aware of cybercrimes.

On another side there is big drawback that our law enforcement agencies are neither knowledgeable nor well equipped for cybercrimes. The law enforcement agencies in our country should be trained. All the cities of our country have not cyber cells. Some investigating officers with the police force may be well equipped to fight cybercrime.

There is legal deficiency in our country against cybercrime. We have dedicated law enforcement agencies which are fully aware of cybercrime. There are very few cybercrime courts where expertise in cybercrime can be utilized. If a law is not enforced with a true spirit, however it is theoretically effective, then it is of no use. Besides this another challenge is that law enforcement machinery is not well equipped to deal with the cyberlaw offenses. Since judiciary is an important part of law so there the savvy judges are needed in courts, who are aware about crime. The officers in the cyber cell should be trained with good technical support and equipments. Judges should also be trained with cyberlaws because the judicial system preserves the law and order in the society.

Various laws on cybercrime and appropriate changes in Indian IT act are needed. Expedition of cybercrime is also needed. Investigating officers of cybercrime should be guided on cyberforensic tools and strategies in our country. Everybody should learn constantly about cybercrime and its ever-growing developments all across the world. It means that a training and orientation on cybercrime for judiciary and the lawyers is needed.

To overcome these challenges there should be workshop or street dramas among the peoples so that the peoples will be aware of cybercrime and it's related laws and acts in our justice system. The conferences and seminars should also be organized in all parts of our country. Some small advertisements and messages should be displayed on televisions or mobiles on cybercrime and it's related frauds.

Q.3. Define the term cybercrime. Give the classification of cybercrime. (R.G.P.V., Nov. 2018)

Ans. **Cybercrime** – Refer to Q.1.

Classification – The classification of cybercrime is as follows –

(i) Cybercrime in Narrow Sense – In this classification, the role of computer is as an object. In this classification the target of the crime is either

information stored on a computer or computer itself. e.g., DDoS attacks, Hacking, Computer sabotage etc.

(ii) Cybercrime in Broad Sense – In this classification, the role of computer is as the environment or context. In this classification a non-substantial role is played by the computer or information stored on the computer, in act of crime. But in this act the computer contain the evidence of crime. e.g., Bank robbery or Murder by using techniques of computers.

Besides this the classification of cybercrime is also done on the basis of different categories of crime. This classification is shown in fig. 1.1.

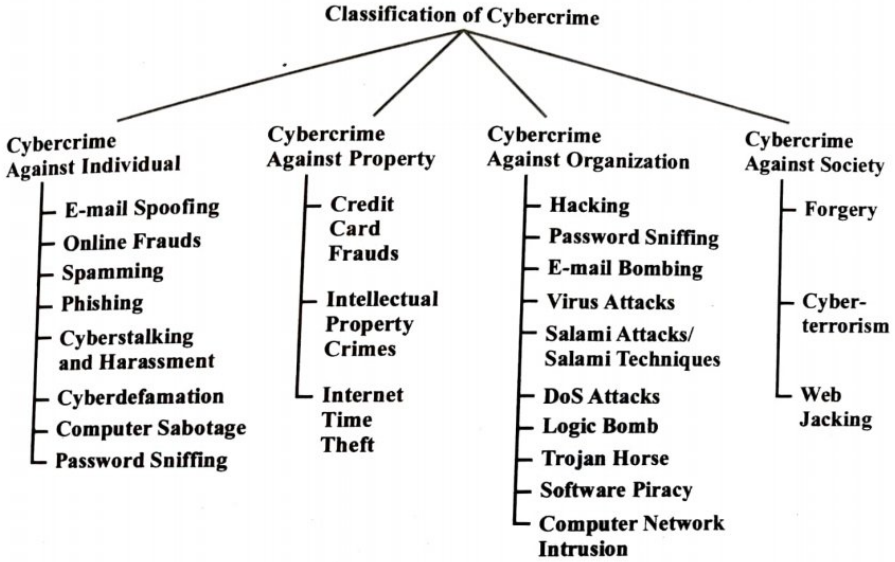


Fig. 1.1 Classification of Cybercrime

Q.4. Explain the categories of cybercrime.

Ans. Categorization of cybercrime is as follows –

(i) Crime Targeted Against Individuals – These kind of crime are exploited because of human weakness like greed and naivety. Financial frauds, sale of non existent items, child pornography, harassment, copyright violation etc. are example of this crime. As the Internet is developing day by day the criminals are exploring them with new tools that are expanded to a large number of victims.

(ii) Crime Targeted Against Property – The stealing of mobile devices is included in this category. Cell phones, laptops, personal digital assistant (PDAs) and removable medias (CDs and pen drives); transmitting harmful programs that can disrupt functions of the systems and/or wipe out the data from hard disk etc., are the examples of this type of crime.

(iii) Crime Targeted Against Organizations – The crime against government/organization include cyberterrorism. In this crime computer tools and Internet are used to terrorize the citizens of a country by stealing or hacking the private information and also to damage the programs.

(iv) Cybercrime as a Single Event – In this crime single attack is performed on the victim's system e.g., opening an attachment that may contain virus and infect the system. This crime includes hacking or fraud.

(v) Cybercrime as a Series of Event – In this crime the attackers attack on victim's system repeatedly.

e.g., interacting with the people/victim on phone and/or via online chat to establish relationship first and then this relationship is exploited to commit the sexual assault.

Q.5. Write a short note on e-mail spoofing. ***(R.G.P.V., Nov. 2018)***

Or

Write short note on IP spoofing.
(R.G.P.V., Dec. 2003, June 2004, Dec. 2010, June 2011)

Or

What do you understand by IP-spoofing ? ***(R.G.P.V., June 2017)***

Or

What do you mean by IP spoofing ? ***(R.G.P.V., Nov. 2019)***

Ans. The most common type of spoofing that you are likely to encounter is IP spoofing, used primarily to spoof the source address of e-mail. In this case, an e-mail message looks like it comes from one address, when in fact it comes from somewhere else instead. The intent is to trick the user into thinking the e-mail comes from a trusted source so that the user will open the e-mail and act on it in some way.

E-mail spoofing can be used to –

(i) Deliver a phishing message (one that cons the user into divulging confidential information). Replying to the e-mail won't work properly, but clicking on links in the e-mail will take the user to a spoofed Web site.

(ii) Deliver a malware payload, such as a virus, worm, or Trojan horse. The malware may come as an attachement that must be downloaded (and perhaps executed) or may be coded into the e-mail so that all the user needs to do is open the e-mail. (The malware installs itself when the e-mail is opened).

One of the more annoying e-mail spoofing tricks is to use the contents of the e-mail address book on a compromised machine as the sources of spoofed e-mail. If you happen to receive an e-mail message, then you know that your address has been harvested and used in that way.

The response generated by the spoofed e-mail was an attempt to deliver a virus. On the target machine the mailer daemon caught the virus and blocked the delivery of the e-mail. The response e-mail was sent to the spoofed address, surprising the recipient because the owner of the spoofed address did not send the e-mail with the attached virus.

A spoofed e-mail is easy to detect by examining the e-mail header information and is something technologically savvy users can be taught to do so. While in other spoofing attacks, we cannot stop the spoofer from sending the spoofed message.

Q.6. What are various ways to avoid e-mail spoofing ?

Ans. If the users of an organization are not enough knowledgeable to understand an e-mail header, then there are some other ways given below that can be used to avoid much of the damage from e-mail spoofing –

(i) Users can be trained to download attachments from untrusted sources. Depending on the nature of organization, the e-mail attachments can be blocked.

(ii) Users of organization should avoid address book software, such as Microsoft Outlook, that is vulnerable to surfing by malware. This can go a long way to prevent the addresses in an address book from being used as spoofed addresses.

(iii) Users can be taught to be skeptical about e-mail that promises something that is too good to be true, even if that e-mail appears to come from a trusted source. The source could be spoofed.

(iv) Remind users frequently that well-known sites like PayPal, Paytm, eBay etc. never ask for confidential information in an e-mail, nor do they provide links in e-mail to pages that ask for such data. If a user wants to change a password/payment option, he or she should use the browser directly.

On the other hand the e-mail server software should be updated frequently, so that it can have most recent virus filters.

Q.7. What do you mean by spamming ? Explain in brief.

Ans. Sometimes it may be not easy to define spam. The process of forging an e-mail with other content without the user's knowledge, is known as spamming, and these types of mails are known as spams. These types of mails are assumed as an example of abuse. Some peoples called these as unsolicited commercial mail. But sometime we desire and feel happy while we get unsolicited mails. Some people called spam as automated commercial mails. But there were many mails that were unsolicited and sometimes automated and not commercial in nature. Hence covering all these aspects we can define spams as unsolicited and automated e-mails.

Since, there is more than 80% use of Internet therefore e-mail spamming affects a large number of Internet users. Because of economic viability spamming is difficult to control. Since there is no amount for operating except management of list, have to pay by the advertisers, so it is difficult to hold senders accountable for their mass mailings. Since the barrier to entry is not so high, the amount of unsolicited mails has increased very much even though these are few spammers. The costs of lost of productivity and fraud for spams are borne by the people and Internet service providers.

Another example of spamming is 'search engine spamming', in which a document is created or altered with the motive to mislead an electronic catalog or filing system. These who are continually attempting to spam a search engine can be excluded from the search index. To be not excluded from web publishing we should avoid the following web publishing techniques –

(i) Keywords should not be repeated

(ii) Keywords should not be used that are not related to the contents on the site.

(iii) There should not be IP cloaking.

(iv) Color text on the same color background should not be used.

(v) There should be no hidden links.

Q.8. How can we avoid spamming ?

Ans. There are several ways to avoid spamming, some of them are as follows –

(i) Limitation of E-mail Address Posted in a Public Electronic Place – Targets of spammers are the e-mail addresses that posted at the bottom of personal web pages. These addresses are harvested by perfect method of cruising the Internet hunting. If we must put personal e-mail on a personal web-page, find a way of disguise it. We should opt out the job, professional that place member e-mail addresses online.

(ii) Stop Ourselves from Filling Out Online forms that Require E-mail Addresses – We should avoid if we can to give our e-mail addresses while we are filling any kind of forms, including online forms that ask for them. We should fill e-mail address only when replies are to be done online.

(iii) Use of E-mail Addresses Not Easy to Guess – We know that passwords can be guessed successfully and now spammer are also trying to guess e-mail addresses. To do this start with sending mails to addresses with short stem personal fields on common ISPs such as Yahoo, Gmail, hotmail etc.

(iv) We should use Multiple E-mail Addresses – We should use one e-mail address for business purpose strictly and multiple e-mail addresses for other purposes. We can use a different e-mail address while filling forms for

nonserious personal business and pleasure. Doing so this will be easy to determine who sells our e-mail addresses. On which form and to whom, which e-mail address was used noting this one can easily track, who is causing spam. Now there are one time disposable e-mail addresses which can used with little efforts.

(v) Spam Filtering – Spam filters should be used either at the network level or application level to block unwanted e-mails always. In both cases the spam is prevented to reach the user by the filter. Many Internet service providers are now offering spam filters.

Q.9. Define the term cyberstalking. How can we tackle this cybercrime?
(R.G.P.V., Nov. 2018, 2019)

Ans. The word cyberstalking has two words – Cyber and stalking. Cyber means the information and communication technologies such as Internet while stalking means the act of watching or following someone for a period of long time. So the cyberstalking combindly defined as the individual or group of individuals uses the communication and information to harass the another person or group of persons. The examples of cyberstalking are as follows –

(i) False accusation

(ii) Monitoring and transmission of threats

(iii) Solicating the minors for sexual purposes

(iv) For harassing someone gathering information about him/her

(v) Damaging the data or equipment.

Cyberstalking also involves the repeated conduction of harassment and threatening by an individual, who uses Internet as communication medium. The most of the victim's of cyberstalking are women and most of the cyberstalkers are men but in some cases are there where the victim are men and the cyberstalker are women.

There are many cases in which cyberstalkers have prior relationship and when the victim want to breakoff this relationship then cyberstalking begins e.g., ex-lover, boss/subordinate, neighbour etc. Cyberstalking can be tackled in the following ways –

(i) We should not leave our personal informations such as – Phone number, address, family background etc. in public places, where anyone could access these informations.

(ii) If stalker wants to establish a connection with victim by making calls or sending e-mails to the victim then it should be reported to the nearest police station or cybercrime cell.

(iii) If stalker is sending repeated e-mails asking for favours do not favour them and report it to the cybercrime cell or police station.

Q.10. Explain the working procedure of cyberstalking.

Ans. There are following ways in which cyberstalking works –

(i) Repeated e-mails are sent to the victim, asking them for various kinds of favour or harassing them.

(ii) The victims are contacted through e-mails by sending them love letters, threatening or can be sexually exploit. The name and mail Id of stalkers may not be actual.

(iii) Cyberstalker collects the personal information of victim, such as address, family details, telephone number of residence as well as office, mobile number e-mail Id etc.

(iv) Stalkers try to establish a connection to victim through mobile/ telephone and if the connection is established they start to make calls to the victim for harassing or threatening them.

(v) The victim's personal information can be posted on any illegal site such as sex worker's service website or dating services etc. They post information as the victim is posting the information and inviting the people to call the victim on the given contact details to have sexual services.

(vi) The people who come across the information, ask the victim for sexual services or relationships by contacting them on given details.

(vii) Since e-mail account of victim is registered on pornographic and sexual sites by the stalker the victim receives the such kind of unsolicited e-mails.

Q.11. What do you mean by Internet time theft ? Explain.

Ans. In these days the use of Internet has become a necessity for everyone. But the Internet time we paid hard money for is being stolen by an unauthorized person then what should we do ? When an unauthorized person uses the Internet hours of another person who has paid for it, then it is called Internet time theft. The unauthorized person gets access to another person's ISP user ID and password either by hacking or by illegal means without that person's knowledge, so this act comes under hacking. Though we can identity time theft if our Internet time has to be recharged frequently while, the use of Internet is infrequent. The Internet time theft is a crime related to the crime conducted through "Identity Theft".

An identity theft involves both theft and fraud, therefore the provisions with regard to forgery as provided under the IPC, 1860 is often invoked along with the IT Act 2000.

The Information Technology Act (IT Act), 2000 is the main act which deals with the lagislation in India for governing cybercrimes. Some sections

of IT 2000 Act dealing with cyber theft are –

(i) Section 43 – If without permission of owner any person damages the computer then he/she shall be liable to pay compensation to the person so affected.

(ii) Section 66 – If any person, dishonestly or fraudulently, does any act referred to in section 43 he/she shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to ₹5 Lakh or with both.

(iii) Section 66B – If a person dishonestly receives stolen computer resource or communication devices shall be liable for punishment with imprisonment for a term which may be extended upto three years or with fine which may extend to rupees one lakh or with both.

(iv) Section 66C – The person who fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may be extended upto three year and shall also be liable to fine which may extended one lakh rupees.

(v) Section 66D – It was inserted to punish cheating by impersonation using computer resources.

Q.12. What is the salami attack ? How information can be gathered through salami technique ? ***(R.G.P.V., Nov. 2018)***

Ans. A fraudlent action by altering of systems for committing financial crimes. These alterations are so insignificant that nobody will notice this. The alterations in the systems can be done by either modification or insertion of malicious program and the main motive of this is financial gain. The salami attack is considered as a minor attack that can be repeated many times.

e.g., a very small amount of money can be stolen from each customer's account in a particular bank. For this purpose the bank employee can modify the program for deducting a small amount from each customer's account every month and doing so the employee will make a sizable amount every month. However the amount will be so small (say ₹1) that no customer will notice this deduction. This type of attack is used for committing financial crimes and it is common and occurs within financial related organizations. Such criminal action will not be noticed by only account holder or customer.

The salami technique can also be used to gather information over a period of time to deduce an overall picture of an organization. The distributed information gather may be of an individual or an organization. A whole database can be built by the data collected from sites, advertisements, documents

collected from trash cons. This data can be intelligent about the target. Since amount of misappropriation is just below the threshold of perception, we need to be more vigilant. Careful examination of our assets, transactions and every other dealing including sharing of confidential information with others might help reduce the chances of an attack by this method.

Q.13. How can we identify the salami attack ? How can the salami attacks be prevented ?

Ans. The only way to detect salami attack is to perform rigorous white box testing, in which each and every line of code which is exhaustive, is checked. This is the only way to identify the salami attack, But this the only way.

A company that protects personal account information has to be on the lookout for individuals who wish to put them in a compromising situation when it comes to another's funds. It is also important to know how to protect this from an angle that is highly sophisticated. Some of the ways to protect this from salami attacks are as follows –

(i) An organization should update the security of the system as high as possible so that attacker could not take advantages of any loophole. By doing so the attacker will not be familiarize with the way the framework designed.

(ii) Banks should also advise customers on reporting any kind of money deduction that they were a part of and that they were not aware. Whether the amount is small or big, the banks should encourage the customers to come forward and openly tell them that this could be an act of fraud.

(iii) The most important thing is that the customers should not store information online ideally, when it comes to bank details. But this fact cannot help that the banks rely on a network that has hooked all customers onto a common platform of transactions that require a database. The safe thing to do is to make sure the bank/website is highly trusted and has not been a part of slanderous past that involved fraud in anyway.

Q.14. Write a short note on cyberdefamation.

Ans. "Harming the reputation of a person either by words that are spoken or intended to be read or by visible representation or by publishing any imputation is said to defame that person".

When the above statement takes place in electronic form then it is called cyberdefamation. It means that when a person is defamed by either using a computer or Internet then it is cyberdefamation.

e.g., A defamatory matter of a person published on web by someone else.

Some laws are formed according to the IPC section 499 regarding defamation are as follows –

(i) If any kind of imputation harm the reputation of that person and is intended to be hurtful to the feeling of his family may be considered as defamation.

(ii) Making an imputation about a company or an association may be considered as defamation.

(iii) The imputations do not harm the person's reputation unless that imputations lowers the moral or intellectual character of that person will not be considered as defamation.

There are two types of defamation, Libel (is written defamation) and slander (is oral defamation).

The words that injure the reputation of person of ordinary intelligence in society will be assumed that it defame the person but if there is no damage to a person's reputation and the person has made allegation of defamation then that person may be held for defamation.

Q.15. Write short notes on the following –

(i) Data diddling

(ii) Forgery

(iii) Newsgroup spam/crimes emanating from usenet newsgroup

(iv) Industrial spying/industrial espionage.

Ans. (i) Data Diddling – The alteration of raw data just before the processing of it by computer, and again changing it back after the processing is completed, is known as data diddling. When private parties computerized their systems, many Electricity Boards in India have been the victims to data diddling programs inserted.

(ii) Forgery – The use of sophisticated computers, printers and scanners can forged the currency notes, postage and revenue stamps. There are many institutes outside, also who are soliciting the sale of fake marksheets or even degree certificates. These marksheets and degree certificates are made using high quality of computers, printers and scanners. Now a days it has become a money growing business involving large monetary amount given to student gangs to exchange for these bogus but authenticate looking certificates.

(iii) Newsgroup Spam/Crimes Emanating from Usenet Newsgroup – Newsgroup spam is a kind of spamming. The term "spam" meant the excessive multiple posting (EMP). Usenet is now more attractive to spammers than ever, because of the invention of Google Groups and its large usenet archive. E-mail spams were actually supported by spamming of usenet newsgroups.

The title "*Global Alert for All : Jesus is coming soon*" was the first recognized usenet spam and it was posted by Clarence L. Thomas IV, a system admin of Andrews University on 18 January 1994.

(iv) Industrial Spying/Industrial Espionage – The corporations also spy on enemy like governments, so the spy is not limited to governments. Better opportunities for espionage are provided by the Internet and privately networked systems. An activity known as "Industrial spying" is abstracting the information above product finances, research and development and marketing strategies. The industrial spy is as old as the industries themselves. Similarly using Internet to achieve this is as old as Internet itself.

Since the Trojans and spyware materials are now becoming available publically, the low-skilled people are now expected to generate high profit our of industrial spying. The aspect of industrial spying will be included to fight against cybercrime.

■■

UNIT 2

WEB JACKING, ONLINE FRAUDS, SOFTWARE PIRACY, COMPUTER NETWORK INTRUSIONS, PASSWORD SNIFFING, IDENTITY THEFT, CYBERTERRORISM, VIRTUAL CRIME

Q.1. What is web jacking ? Explain with example.

Ans. The name web jacking is derived from hijacking. This method is used in social media where hacker takes control of a website fraudulently. It can be done by either changing the content of the original site or even redirect the user to another fake similar looking page controlled by him. In web jacking the owner of the website has no control and the attacker may use the website for his own selfish interest or for fulfilling political objectives for money. There are many cases where the attacker has asked for ransom and even posted obscene material on the site. A clone of the website can be created by using the web jacking method and it can be presented to the victim with the new link saying that the site has moved.

When we have our cursor over the link provided, the URL presented will be the original one, and not the attacker's site. But when we click on the new link, it open and is quickly replaced with the malicious web server. Here the name of the site on the address bar will be slightly different from the original website, that can trick the users into thinking it's a legitimate site e.g., '*gmail*' may direct us to 'gmail', where *l* is replaced by 1. Obviously it can be looked that it's not "gmail.com" but people still click the web.

Web jacking can also be done by sending a counterfeit message to the registrar controlling the domain name registration, under a false identity asking him to connect a domain name to the web jacker's. Thus, IP address sending unsuspecting consumers who enter that particular domain name to a website controlled by the web jacker. The purpose of this attack is to try gain the credentials such as user names, passwords and account numbers of users by using fake web page with a valid link which opens when the user is redirected to it after opening the legitimate site.

e.g., an example of web jacking is, messages are sent to people by making believe them that they have won lottery and to claim to this amount they are asked to click the link where a form is opened after clicking that link. In this form all personal information like name, address, mobile number, office telephone number, account and other related informations are asked and thus using these informations the attackers hacks their bank account.

Q.2. Discuss the method of web jacking in detail.

Ans. The web jacking attack vector is a phishing technique that can be used in social engineering engagements. A fake website is created by using this method, and when the victim opens the link a page appears with the message that the website has moved and they need to click another link. If the victim clicks the link he will be redirected to a fake page that looks real.

This kind of attack has already been included in Social Engineering Toolkit (SET). So now we shall use the SET to implement this method in the following steps –

Step-1 – Firstly we shall open SET and select the option 2 which is the website attack vectors, as shown in fig. 2.1.

```
Select from the menu;

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-based Attack Vector
   7) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) QR Code Generator Attack Vector
  10) Third Party Modules

  99) Return back to the main menu.

set>2
```

Fig. 2.1 Social Engineering Toolkit

Step-2 – Now in website attack vectors we see a list with available web attack methods. Here we are going to select option 6 which is web jacking attack. The list of website attack vectors is shown in fig. 2.2.

```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Man Left in the Middle Attack Method
   6) Web Jacking Attack Method
   7) Multi-Attack Web Method
   8) Victim Web Profiler
   9) Create or Import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack>6
```

Fig. 2.2 Website Attack Vector

Step-3 – Now in web jacking attack menu we have three options –

(i) Web templates (ii) Site cloner (iii) Custom import.

Here we will select the site cloner in order to clone the website of our interest. Note that this type of attack works with the credential harvester method so we need to choose a website that has username and password field. Template of web jacking attack is shown in fig. 2.3.

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[*] SET supports both HTTP and HTTPS
[*] Example : http://www.thisisafakesite.com
set:webattack>Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit....

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

Press {return} to continue.
```

Fig. 2.3 Web Jacking Attacks

Step-4 – Now for site cloning we choose the site with username and password credentials. For this purpose we can select facebook because of it's popularity in which are moved to the link of new website. Now it is the time to send our link with our IP address to the victim. Let's see what the victim will see if he opens the links, as shown in fig. 2.4.

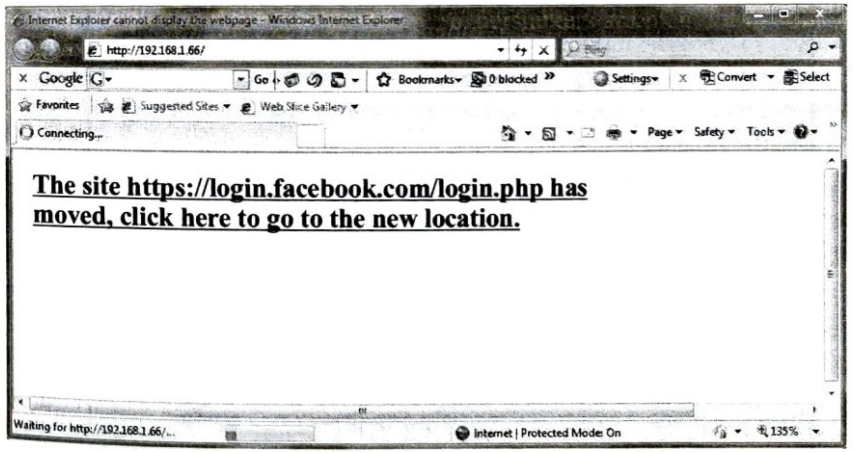


Fig. 2.4 Site Cloning

Step-5 – As we can see a message will appear informing the user that the website has moved to a new location. The link on the message seems valid so any unsuspicious users will click on the link. At that time a new page will load into the victim's browser which will be fake and is running on clone web server as shown in fig. 2.5.

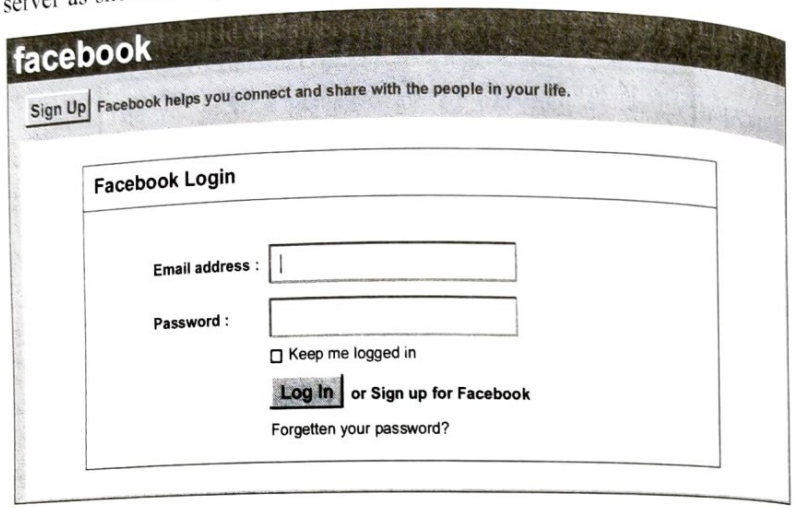


Fig. 2.5 Fake Facebook Page

Step-6 – If the victim enters his credentials into the facebook page that looks like real one then the attacker will be able to capture his username and password as shown in fig. 2.6.

```
[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link
[*] Social Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below :
172.16.56.128 - - [23/Mar/2012 14:42:17] *GET/HTTP/1.1" 200-
Blackbox.home - - [23/Mar/2012 14:46:01] *GET/HTTP/1.1" 200-
Blackbox.home - - [23/Mar/2012 14:46:06] *GET/index2.html HTTP/1.1"200-
[*] WE GOT A HIT: Printing the output :
PRAM : post_form_id bedf6447a24eea6465074ce20cedc88f
PRAM : lsd=Qww5z
PRAM : return_session=0
PRAM : legacy_return=1
PRAM : display=
PRAM : session_key_only=0
PRAM : trynum=1
PRAM : charset_test=€, ', €, ', *, ' Ą,€
PRAM : lsd=Qww5z
PRAM : timezone=0
PRAM : lgnrnd=074137_I-GY
PRAM : lgnjs=1332513966
POSSIBLE USERNAME FIELD FOUND : email=test@pentestlab.wordpress.com
POSSIBLE PASSWORD FIELD FOUND : pass=letmein
PRAM : defalt persistent=0
[*] WHEN YOU'R FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Fig. 2.6 Capturing the Credentials

Q.3. Write a short note on online frauds.

Ans. Hacking involves a few major types of crimes such as website spoofing, e-mail security alerts etc. The authentic looking websites that are known as spoof are created in spoofing website and e-mail security threats. These websites make user to enter personal details which will be used by attacker to access business and bank accounts. This type of online fraud is common in banking and financial sector. There are number of organizations who receive e-mails which usually has a link to spoofed website. In these e-mails people are asked to enter the user Id and password on spoofed website so the hackers can retain these information. So we should not provide our sensitive information like bank account details on these sites even if the page seems legitimate.

It may be possible in virus hoax e-mails that warnings are genuine, so there is always a confusion that we should take it lightly or seriously. A good solution that we should go first by visiting an antivirus site such as McAfee or other before taking any action.

Sometimes users get lottery messages on e-mails or letter that he/she has won the lottery. To claim the amount of lottery the personal information such as name, address, bank account number, mobile number, etc. are asked from users, so that money can be directly transferred to customers' account. Then banking details are used for other frauds and scams.

Q.4. Write a short note on software piracy. ***(R.G.P.V., Nov. 2018)***

Or

What do you mean by software piracy ? ***(R.G.P.V., Nov. 2019)***

Ans. The illegal copying, distribution or use of software is known as software piracy. Since it is such a profitable business that it has caught the attention of organized crime groups in a number of countries. The act of stealing software that is legally protected is also known as software piracy. It was shocking that in 2006 the 35% of softwares in all over the world were illegal. This was amounted to about $40 billion loss due to software piracy.

When we purchase a commercial software package, an end user license agreement (EULA) is included to protect that software program from copyright infringement. In the terms and conditions of license it is stated that we can install the original copy of software bought on one computer and that we can make a backup copy in case the original is lost or damaged.

Software piracy mainly applied to full-function commercial softwares. The function-restricted or time-limited versions of commercial software are not pirated because they are freely available. Similarly the softwares that are copyrighted but freely available at no charge called 'freeware' are also not pirated.

Q.5. Explain the types of software piracy. Also discuss the dangers of software piracy.

Ans. The variety of pirating techniques explains how some individuals pirate softwares according to their need. The types of software piracy are as follows –

(i) Softlifting – It is a most common type of software piracy. It is a variety of software piracy in which someone purchases one version of the software and downloads it onto multiple computers, however according to software license terms it should be downloaded only once. This type of software piracy often occurs in school or business environments and here usually the motive is to save money.

(ii) Client-server Overuse – When many people on a network use one main copy of the program at the same time, then it is called client-server overuse. This often occurs when businesses are on a local area network and download the softwares for all employess to use. This becomes software piracy if the license does not entitle us to use it multiple times.

(iii) Hard Disk Loading – In this type someone buys a legal version of the software and then copies or installs it onto computer hard disks, and sells the product.

(iv) Counterfeiting – When computer programs are illegally duplicated and sold with the appearance of authenticity then counterfeiting occurs. The counterfeit softwares are sold at low prices in compare of legitimate software.

(v) Online Piracy – When illegal software is sold shared or acquired by means of the Internet then it is called online piracy or Internet piracy. This is usually done through a peer-to-peer (P2P) file sharing system, which is usually found in the form of online auction sites and blogs.

The dangers of software piracy are as follows –

(i) There are a lot of chances that the software will malfunction or fail.

(ii) Forfeited access to support for the program such as training, upgrades, customer support etc.

(iii) No warranty and software cannot be updated.

(iv) Increased risk of infecting PC with malware, viruses or spyware.

(v) PC can be slow down.

(vi) Legal action due to copyright infringement.

Q.6. What is intrusion ?

Ans. An intrusion is a deliberate unauthorized attempt, successful or not, to break into, access, manipulate, or misuse some valuable property and where the misuse may result into or render the property unreliable or unusable. The person who intrudes is an intruder.

Q.7. What is intruder ? Explain three classes of intruders. ***(R.G.P.V., Dec. 2017)***

Or

Explain the 3 classes of intruder. ***(R.G.P.V., Dec. 2006, 2012)***

Or

What is an intruder ? Describe its classification. (R.G.P.V., Dec. 2015)

Ans. One of the two most popular threats to security is the intruder (the other is viruses), generally referred to as a *hacker* or *cracker*. An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system, is known as ***intruder***. There are three classes of intruders –

(i) Masquerader – An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

(ii) Misfeasor – A legitimate user who accesses data, programs or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

(iii) Clandestine User – An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Q.8. List and briefly define three classes of intruders. What are two common techniques used to protect a password file ? ***(R.G.P.V., June 2005, Dec. 2011)***

Ans. **Three Classes of Intruders** – Refer to Q.7.

Techniques Used to Protect a Password File – One way to thwart a password attack is to deny the opponent access to the password file. If the encrypted password portion of the file is accessible only by a privileged user; then the opponent cannot read it without already knowing the password of a privileged user; but this approach has several drawbacks. A more effective strategy would be to force users to select passwords that are difficult to guess.

Q.9. What is an intrusion detection system (IDS) ?

Or

Discuss the concept of intrusion detection system. (R.G.P.V., Nov. 2019)

Ans. An ***intrusion detection system (IDS)*** is a system used to detect unauthorized intrusions into computer systems and networks. Intrusion detection as a technology is not new, it has been used for generations to defend valuable resources. Kings, emperors, and nobles who had wealth used it in rather an interesting way. They built castles and palaces on tops of mountains and sharp cliffs with observation towers to provide them with a

clear overview of the lands below where they could detect any attempted intrusion ahead of time to defend themselves.

Over the years, intrusion detection has been used by individuals and companies in a number of ways including erecting ways and fences around valuable resources with sentry boxes to watch the activities surrounding the premises of the resource. Individuals have used dogs, flood lights, electronic fences, and closed circuit television and other watchful gadgets to be able to detect intrusions.

As technology has developed, a new industry based on intrusion detection has sprung up. Security firms are cropping up everywhere to offer individual and property security–to be a watchful eye so that the property owner can sleep or take a vacation in peace. These new systems have been made to configure changes, compare user actions against known attack scenarios, and be able to predict changes in activities that indicate and can lead to suspicious activities.

Q.10. Discuss the best approaches to implementing an effective IDS.

Or

Explain statistical anomaly and rule-based detection technique of intrusion detection. ***(R.G.P.V., Dec. 2017)***

Or

Clearly differentiate between anomaly detection and signature detection techniques of IDS. ***(R.G.P.V., June 2017)***

Ans. The following approaches are used to implement an IDS –

(i) Anomaly Detection – Anomaly based systems are *learning* systems in a sense that they work by continuously creating norms of activities. These norms are then later used to detect anomalies that might indicate an intrusion. Anomaly detection compares observed activity against expected normal usage profiles *learned*. The profiles may be developed for users, groups of users, applications, or system resource usage.

In anomaly detection, it is assumed that all intrusive activities are necessarily anomalous. It happens in real life too, where most *bad* activities are anomalous and we can, therefore, be able to character profile the *bad elements* in society. The anomaly detection concept, therefore, will create, for every guarded system, a corresponding database of *normal* profiles. Any activity on the system is checked against these profiles and is deemed acceptable or not based on the presence of such activity in the profile database.

Areas of interest are threshold monitoring, user work profiling, group work profiling, resource profiling, executable profiling, static work profiling, adaptive work profiling, and adaptive rule base profiling.

Anonymous behaviours are detected when the identification engine takes observed activities and compares them to the rule-base profiles for significant

deviations. The profiles are commonly for individual users, groups of users, system resource usages, and a collection of others as discussed below –

(a) Individual Profile – This is a collection of common activities a user is expected to do and with little deviation from the expected norm. This may cover specific user events like the time being longer than usual usage, recent changes in user work patterns, and significant or irregular user requests.

(b) Group Profile – This profile covers a group of users with a common work pattern, resource requests and usage, and historic activities. It is expected that each individual user in the group follows the group activity patterns.

(c) Resource Profile – This includes the monitoring of the use patterns of the system resources like applications, accounts, storage media, protocols, communications ports, and a list of many others the system manager may wish to include. It is expected, depending on the rule-based profile, that common uses will not deviate significantly from these rules.

(d) Other Profiles – These include executable profiles that monitor how executable programs use the system resources. This, for example, may be used to monitor strange deviations of an executable program if it has an embedded Trojan worm or a trapdoor virus. In addition to executable profiles, there are also the following profiles – work profile which includes monitoring the ports, static profile whose job is to monitor other profiles periodically updating them so that those profiles, cannot slowly expand to sneak in intruder behaviour, and a variation of the work profile called the adaptive profile which monitors work profiles, automatically updating them to reflect recent upsurges in usage. Finally there is also the adaptive rule base profile which monitors historic usage patterns of all other profiles and uses them to make updates to the rule-base.

Beside being embarrassing and time consuming, the concept also has other problems. If we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, then two problems arise –

(a) Anomalous activities that are not intrusive are classified as intrusive.

(b) Intrusive activities that are not anomalous result in false negatives, that is, events are not flagged intrusive, though they actually are.

Anomaly detection systems are also computationally expensive because of the overhead of keeping track of, and possibly updating, several system profile metrics.

(ii) Misuse Detection – The misuse detection concept assumes that each intrusive activity is representable by a unique pattern or a ***signature*** so that slight variations of the same activity produce a new signature and therefore can also be detected. Misuse detection systems, are therefore, commonly

known as ***signature systems.*** They work by looking for a specific signature on a system. Identification engines perform well by monitoring these patterns of known misuse of system resources. These patterns, once observed, are compared to those in the rule-base that describe *bad* or *undesirable* usage of resources. To accomplish this, a knowledge database and a rule engine must be developed to work together. Misuse pattern analysis is best done by expert systems, model based reasoning, or neural networks.

The major problems arise out of this concept are as follows –

(a) The system cannot detect unknown attacks with unmapped and un-archived signatures.

(b) The system cannot predict new attacks and will, therefore, be responding after an attack has occurred. This means that the system will never detect a new attack.

Q.11. Explain the following terms – Masquerader, Misfeasor, Clandestine user and Base-rate fallacy. Explain statistical anomaly detection method for intrusion detection. ***(R.G.P.V., June 2010)***

Ans. **Masquerader, Misfeasor and Clandestine User** – Refer to Q.7.

Base-rate Fallacy – To be of practical use, an intrusion detection system should detect a substantial percentage of intrusions while keeping the false alarm rate at an acceptable level. If only a modest percentage of actual intrusions are detected, the system provides a false sense of security. On the other hand, if the system frequently triggers an alert when there is no intrusion (a false alarm) then either system managers will begin to ignore the alarms, or much time will be wasted analyzing the false alarms.

Unfortunately, because of the nature of the probabilities involved, it is very difficult to meet the standard of high rate of detections with a low rate of false alarms. In general, if the actual numbers of intrusions is low compared to the number of lagitimate users of a system, then the false alarm rate will be high unless the test is extermely discriminating. A study of existing intrusion detection systems, indicated that current systems have not overcome the problem of the base-rate fallacy.

Anomaly Detection Method – Refer to Q.10 (i).

Q.12. Describe various types of intrusion detection systems. ***(R.G.P.V., Dec. 2016)***

Or

Give different types of intrusion detection systems. (R.G.P.V., June 2016)

Ans. Intrusion detection systems can be classified based on their monitoring scope. That is, those that monitor only a small area and those that can monitor a wide area. Those that monitor a wide area are called as network-based intrusion detection and those that have a limited scope are called as host-based detections.

(i) Network-based Intrusion Detection Systems (NIDSs) – Network-based intrusion detection systems have the whole network as the monitoring scope. They monitor the traffic on the network to detect intrusions. They are responsible for detecting anomalous, inappropriate, or other data that may be considered unauthorized and harmful occurring on a network. There are striking differences between NIDS and firewalls. Firewalls are configured to allow or deny access to a particular service or host based on a set of rules. Only when the traffic matches an acceptable pattern is it permitted to proceed regardless of what the packet contains. An NIDS also captures and inspects every packet that is destined to the network regardless of whether it's permitted or not. If the packet signature, based on the contents of the packet is not among the acceptable signatures, then an alert is generated.

There are many ways an NIDS may be run. It can either be run as an independent standalone machine where it promiscuously watches over all network traffic or it can just monitor itself as the target machine to watch over its own traffic. For example in this mode, it can watch itself to see if someone is attempting a SYN-flood or a TCP port scan.

While NIDSs can be very effective in capturing all incoming network traffic, it is possible that an attacker can evade this detection by exploiting ambiguities in the traffic stream as seen by the NIDS. Mark Handley, Vern Paxson, and Christian Kreibich list the sources of these exploitable ambiguities as follows –

(a) Several NIDSs do not have complete analysis capabilities to analyze a full range of behaviour that can be exposed by the user and allowed by a particular protocol. The attacker can also evade the NIDS even if the NIDS does perform analysis for the protocol.

(b) Since NIDSs are far removed from individual hosts, they do not have full knowledge of each host's protocol implementation. This knowledge is necessary for the NIDS to be able to determine how the host may treat a given sequence of packets if different implementations interpret the same stream of packets in different ways.

(c) Again, since NIDSs do not have a full picture of the network topology between the NIDS and the hosts, the NIDS may be unable to determine whether a given packet will even be seen by the hosts.

(ii) Host-based Intrusion Detection Systems (HIDS) – Host-based intrusion detection is the technique of detecting malicious activities on a single

computer. A host-based intrusion detection system, is therefore, deployed on a single target computer and it uses software that monitors operating system specific logs including system, event, and security logs on Windows systems and syslog in Unix environments to monitor sudden changes in these logs. When a change is detected in any of these files, the HIDS compares the new log entry with its configured attack signatures to see if there is a match. If a match is detected then this signals the presence of an illegitimate activity.

Although HIDSs are deployable on a single computer, they can also be put on a remote host or they can be deployed on a segment of a network to monitor a section of the segment. The data gathered, which sometimes can be overwhelming, is then compared with the rules in the organization's security policy. The main problem with HIDSs is that given the amount of data logs generated, the analysis of such raw data can put significant overhead not only on the processing power needed to analyze this data but also on the security staff needed to review the data.

Host sensors can also use user level processes to check key system files and executables to periodically calculate their checksum and report changes in the checksum.

Q.13. What do you mean by intrusion ? Explain types of IDS detection techniques. ***(R.G.P.V., Dec. 2013)***

Ans. Refer to Q.6 and Q.12.

Q.14. What is an IDS ? Explain the different types of IDS in brief. ***(R.G.P.V., Dec. 2010, June 2011)***

Ans. Refer to Q.9 and Q.12.

Q.15. Explain the architecture of a distributed intrusion detection system. Give the major issues in the design. ***(R.G.P.V., June 2012)***

Ans. **Architecture of a Distributed Intrusion Detection System** – The architecture of a distributed intrusion detection system consists of three main components as shown in fig. 2.7.

(i) Host Agent Module – An audit collection module operates as a background process on a monitored system. Its aim is to gather data on security related events on the host and send these to the central manager.

(ii) LAN Monitor Agent Module – It operates in the same manner as a host agent module except that it analyzes LAN traffic and sends the results to the central manager.

(iii) Central Manager Module – It gets reports from host agents and LAN monitor and processes and correlates these reports to detect intrusion.

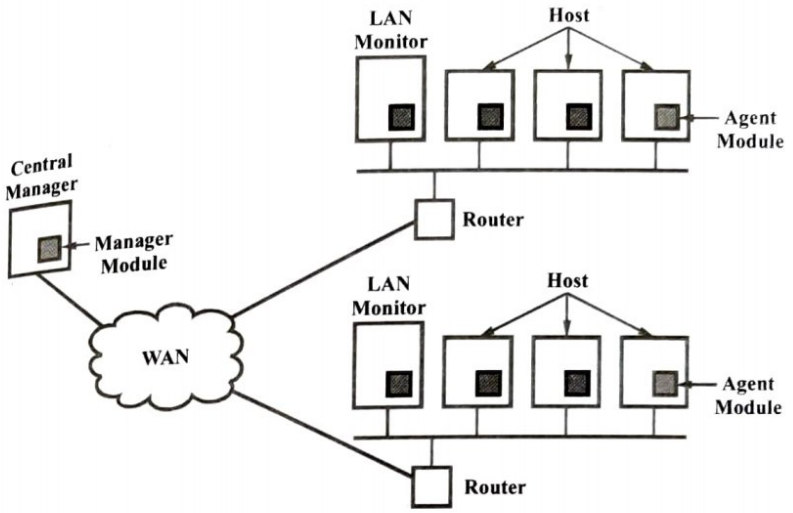


Fig. 2.7 Architecture for Distributed Intrusion Detection

Major Issues in the Design of a Distributed Intrusion Detection System – The following are the major design issues in a distributed intrusion detection system –

(i) The architecture can be either centralized or decentralized. There is a single central point of collection and analysis of all audit data in a centralized architecture. This simplifies the task of correlating incoming reports but creates a potential bottleneck and single point of failure. On the other extreme, there are more than one analysis centers in a decentralized architecture, but these must coordinate their activities and exchange information.

(ii) There is one or more nodes in the network that will serve as collection and analysis points for the data from the systems on the network. Therefore, either raw audit data or summary data must be sent across the network. Hence, there is a need to assure the integrity and confidentiality of these data. Integrity is needed to prevent an intruder from masking his or her activities by altering the transmitted audit information. Confidentiality is needed because the transmitted audit information could be valuable.

(iii) A distributed intrusion detection system may require to deal with different audit record formats. In a heterogeneous environment, different systems will use different native audit collection systems and, if using intrusion detection, may use different formats for security-related audit records.

Q.16. What are file system indications for a possible intrusion ?

Ans. File system has new file and directories, missing files, altered file data, MDS sum or shalsummismatches, new getuid programs and rapidly growing or overflowing file systems.

New Files and Directories – There can be file with bad digital signatures and multiple new file and directoreis. File name will be very suspicious like starting with one or more dots and legitimate-sounding file name appearing in unappropriate places.

Missing Files – Some type of difficulties indicated by missing files particularly log files.

Setuid and Setgid Programs – New set uid and set gid files are a right place to start looking the problems.

Rapidly Changing Filessystem Sizes – Rapidly changing file system sizes may be a sign of a hacker's monitoring program producing large logfiles.

Update Public File Archives – Check the contenrs of your web and FTP areas for updated files.

Q.17. Discuss the various intrusion detection tools. (R.G.P.V., June 2012)

Or

Briefly explain available tools of intrusion detection.

(R.G.P.V., Dec.2016)

Ans. Intrusion detection tools work best when used after vulnerability scans have been performed. They then stand watch. Table 2.1 shows various current ID tools.

Table 2.1 Some Current ID Tools

Name	*Source*
Realsecure v.3.0	ISS
Net Perver 3.1	Axent Technologies
Net Ranger v2.2	CISCO
FlightRemohe v2.2	NFR Network
Sessi-Wall-3, v4.0	Computer Associates
Kane Security Monitor	Security Dynamics

All network-based intrusion detection tools can provide recon (reconaince) probes in addition to port and host scans. As monitoring tools, they give information on –

(i) Hundreds of thousands of network connections
(ii) External break-in attempts
(iii) Internal scans
(iv) Misuse patterns of confidential data
(v) Unencrypted remote logins or a Web sessions
(vi) Unusual or potentially troublesome observed network traffic.

All this information is gathered by these tools monitoring network components and services that include –

(i) Servers for
(a) Mail (b) FTP (c) Web activities.
(ii) DNS, RADIUS and others
(iii) TCP/IP ports
(iv) Routers, bridges, and other WAN connection
(v) Drive Space
(vi) Event log entries
(vii) File modes and existence
(viii) File contents.

In addition to the tools in table 2.1 several other commercial and freeware IDS and scanning tools can be deployed on a network to gather these probes. The most common are as follows –

(i) Flow-tools – A software package for collecting and processing NetFlow data from Cisco and Juniper routers.

(ii) Tripwir – Monitors the status of individual files and determines whether they were changed.

(iii) TCPdump – A freeware and one of the most popular IDS tool created by National Research Group.

(iv) Snort – Another freeware and popular intrusion detection system that alerts and reassembles the TCPdump format.

(v) Portsentry – A port scan detector that shuts down attacking hosts, denying them access to any network host while notifying administrators.

(vi) Dragon IDS – Developed by Network Security Wizards, Inc.it is a popular commercial IDS.

(vii) TCP Wrappers – Logs connection attempts against protected services and evaluates them against an access control list before accepting the connection.

(viii) RealSecure – By Internet Security System (ISS). Very popular IDS.

(ix) Shadow – The oldest IDS tool. It is also a freeware.

(x) NetProwler – An intrusion-detection tool that prevents network intrusions through network probing, system misuse, and other malicious activities by users.

(xi) Network Auditor – It gives the power to determine exactly what hardware and software is installed on the network and checks this for faults or changes.

Q.18. What are the different methods of evading IDSs ?

Ans. IDSs can be thwarted or bypassed by a number of methods. The principal methods used are –

(i) Session Splicing – In session splicing, the data to be delivered for the attack is spread out over multiple packets, thus making it more difficult for pattern matching techniques to detect an attack signature. Session splicing is characterized by a steady stream of small packets. Tools such as Nessus and Whisker incorporate session splicing methods.

(ii) Fragmentation Overlap – This approach attempts to foil an IDS by transmitting packets in a fashion that one packet fragment overwrites data from a previous fragment. The information in the packets is organized such that when the packets are reassembled, an attack string is sent to the destination computer.

(iii) Fragmentation Overwrite – In this fragmentation attack, the total fragment data of one packet overwrites a previous fragment. When the target host assembles the fragments, an attack string results.

(iv) Denial of Service – A DoS attack against an IDS attempts to flood the IDS so that it cannot function properly. The IDS will be consumed with the overwhelming traffic, allowing malicious code to slip through. Another effect is that a large number of alarms will be generated that cannot be processed by the alarm handling management systems.

(v) Insertion – In an insertion attack, an IDS accepts a packet and assumes that the host system will also accept and process the packet. In fact, the host system will reject the packet. The IDS will, then, accumulate attack strings that will exploit vulnerabilities in the IDS and, for example, contaminate the signatures used in signature analysis.

(vi) Evasion – An evasion attack is the opposite of an insertion attack in that a packet is rejected by an IDS, but accepted by the host system. Because the IDS rejects the packet outright, it does not checks the packet contents. The packet can contain data that is used to exploit the host system.

(vii) Obfuscating Attack Payload – If the attack payload in a packet is encoded or obfuscated, the IDS will not recognize the payload as an attack and pass it on the server for decoding. For example, the attack data could be encoded with Unicode.

(viii) Polymorphic Code – If a continually changing signature is generating by encoding the attack payload with a polymorphic code, this signature would not match a signature in the attack signature database.

Q.19. Write short note on sniffing. ***(R.G.P.V., Dec. 2003, June 2004)***

Or

What is sniffing ? ***(R.G.P.V., Dec. 2015)***

Ans. Sniffing is the act of collecting packets from a network connection using either a special application or a piece of hardware called a *sniffer.* A sniffer takes a copy of and displays all of the traffic a network card sees. When implemented correctly, a sniffer is completely passive, having no effect on the traffic. Except for the fact that it takes processing time and memory, a sniffer should have no effect on its host computer. Ethereal, Ettercap, and Packetyzer are some popular sniffers that allow for traffic collection, analysis, and TCP stream reconstruction. Traffic collection refers to the sniffer's ability to receive a copy of network traffic. Traffic analysis is the sniffer's ability to break out relevant fields (such as IP address) from the captured packets. A sniffer with good traffic analysis capabilities can easily be display specified fields within the packet. It will also be able to recognize many different types of packets. Some even have the capability to analyze proprietary packet types. TCP stream reconstruction is the process by which a sniffer captures and reconstructs an entire TCP stream so that the user can see and analyze the traffic in an easy-to-understand manner. Some sniffers allow for almost complete stream reconstruction. They can pull out the data that is being passed within the traffic. This allows reconstruction of the sequence of mail commands that is passed between a mail host and a client, thus enabling debugging of the higher level protocols. For instance, SMTP could be debugged with the help of a sniffer. Sniffing is done for many reasons, with two of the most common being network performance analysis (boring) and spying. Sniffing will be used as a tool to further our spying capability.

Q.20. What are the types of sniffing ?

Ans. Protocol analyzers or packet sniffers come in two types – general and attack. A general packet sniffer captures all packets and sometimes has diagnostic tools to help you examine and troubleshoot packet contents and connections. There are many free software versions of these types of sniffers available. One of my favourite free sniffers is WireShark. An attack sniffer, on the other hand, is a modified form of a general packet sniffer. An attack sniffer is only looking for certain kinds of packets, like the authentication information in telnet packets, or credit card information in HTTP connections. Basically, the attacker has modified the software of a general sniffer to capture specific kinds of traffic that will be useful for other types of attacks.

Q.21. Write a short note on password sniffing. ***(R.G.P.V., Nov. 2018)***

Ans. Password sniffing is an attack on the Internet that is used to steal username and password from the network. It was the worst security problem

on the Internet in 1990s. In 1990s every week there was a news about password sniffing attack. Since now-a-days strong encryption is used for protecting passwords, so it was mostly of historical interest.

Password sniffing can also be termed as network sniffing. It is act of intercepting, monitoring and capturing of data packets in traffic of a network, especially in Local Area Network (LAN). The motive of network sniffing is to steal information such as usernames, passwords, network messages etc. in form of packets using a sniffer software program like wireshark. Another mean of passive attack is network sniffing, to abstract useful information like Internet Protocol (IP) address ranges, hidden servers or networks, and other available services on the system or network.

The password sniffing problem was mostly solved by SSH, which replaced several prior insecure protocols. Hashing of passwords or encryption has also been introduced by many other protocols, which makes password sniffing attack less practical. Even then various other credentials stealing and replay attacks are still widely used. Man-in-the-middle attack is being commonly used for stealing passwords and credentials today.

Q.22. How can the password sniffing be implemented ? What are the complications of password sniffing ?

Ans. The typical implementation of a password sniffing attack involves gaining access to a computer connected to a local area network and installing a password sniffer on it. The password sniffer is a small program that listens to all traffic in the attached network(s), builds data streams out of TCP/IP packets, and extracts user names and passwords from those streams that contain protocols that send cleartext passwords.

In network sniffing attack, the data from each TCP/IP stream can be separated and the information can be extracted from them. It is not difficult attack to code.

This attack can also be applied on switches, routers and printers. Now-a-days it is common for attackers to install presence on such devices. They don't run antivirus and are not easy to audit. Since, traffic naturally goes through switches and routers, so no extra network packets need to be sent to fool switches into sending traffic of interest to the listening node.

Complications of Password Sniffing – Many developments have made password sniffing difficult besides adding encryption. Even though the encryption is the only reliable solution, and due to main-in-the-middle attack risks, the encryption must include proper authentication of communicating parties.

In 1990s every host was able to see all traffic in the network because of thick ethernet cable that was common at that time. So it was enough to put a network interface into casual mode to see all traffic. Switches and star-like topologies are used by networks today, which make this more difficult. However, it is possible to fool switches to send traffic to any host, or perform the attack on the switch itself.

MAC addresses for each network port in switches are hard-coded by some enterprises and updates and passwords are set on switches. Some configurations make this attack difficult. However, it is impossible to control all switches and routers on long-distance connections.

Q.23. What do you mean by identity theft ?

Ans. When someone claims to be someone else to steal money or get other benefits then this fraud is referred to as identity theft. When someone else's identity is used by a criminal or a fraud person then this theft occurs. The person, can face various problems when he/she is held responsible for the criminal's action, whose identity is used. For personal gain using another person's id is declared as crime by some specific levels, in many countries. In India, it is also a punishable offense under the section 66C and section 66D under Indian IT Act.

A non-profit organization was formed in the US, with the objective to support the society for spreading awareness about ID theft fraud because of it's severity. This organization was named as Identity Theft Resource Center (ITRC).

In 2010, a report was published by Javelin strategy in his research paper that the number of identity fraud victims were increased by 12% during 2009, and amount of fraud increased by 12.5%.

The statistics was provided by Federal Trade Commission (FTC) about the identity fraud in which prime frauds was mentioned is given below –

(i) Loan Fraud – The loan fraud was 5% at that time. When a loan is applied on victim's name by attacker then this fraud occurs.

(ii) Government Fraud – There are 9% of government frauds which include SSN, driving license and income tax fraud.

(iii) Employment Fraud – There are 12% of employment frauds where the attacker borrows the victim's valid SSN.

(iv) Bank Fraud – Besides credit card frauds, ATM and cheque frauds have been reported. There are 17% of bank frauds.

(v) Credit Card Frauds – There are 26% of credit card frauds. These are highest rated frauds. In this fraud the victim's credit card number is acquired by someone else and used for making purchase.

Q.24. What a person can do to protect himself/herself from identity theft ? ***(R.G.P.V., Nov. 2018)***

Ans. Since our identity and/or personal informations are displayed on the internet evereytyme, so we can be a victim of identity theft or fraud. Hence Internet users should erase their identity and/or protect their ID, i.e. every information about them, available on the Internet. Since, it is impossible to get a tool that erase all informations completely from the Internet, so a person can do the following to protect himself/herself from identity theft –

(i) Monitoring of Credit – The information about our credit account and bill payment history are contained in the credit report, so someone can impersonate us. So we should aware for suspicious signs. The identity protection services, can also be used for extra security, which ranges in credit monitoring to database scanning.

(ii) Using Update Web Browser – An update web browser should be used everytime to make sure that we are taking advantage of its current safety features.

(iii) Keeping Records of Financial Data and Transactions – Our statements should be reviewed time to time for any activity and change that we have not made.

(iv) Installing Security Software – We should install antivirus and antispyware softwares, and keep these security softwares upto date as a safety measure against online intrusions.

(v) Storing Sensitive Data Securely – We should keep our online sensitive information secured. We can store these online information sucurely by using file encryption software.

(vi) Protecting Our Personally Identifiable Information – We should not provide our personally identifiable information to any other person. We should provide these informations after finding out that why the information is needed and it is needed to provide or not. We should carefully share our personal information on social networking sites.

(vii) Staying Alert to the Latest Scams – We should be aware to protect against fraud. We should also create awareness in our family and surroundings by sharing security tips with everyone.

Q.25. Write a short note on personally identifiable information (PII).

Ans. The attacker always try to find the information by using which a single person can be located, contacted or identified or by using which a single individual can be uniquely identified out of other sources. Personally identifiable information is based on four common types viz., personal, personally, identifiable and identifying.

The elements given below are attempted to be stolen. These elements can express the purpose of distinguishing individual identity –

(i) Full name of user
(ii) Residence and office telephone number and mobile number
(iii) PAN card number
(iv) Credit/Debit card number
(v) D.O.B.
(vi) Driver's license number
(vii) E-mail address/Online account details etc.

The personally identifiable information can also be divided into two categories as –

(i) Classified Information – The subcategories of classified information are –

(a) Secret – National security policies, military plans etc. are secret informations. The disclosure of these informations can damage the national security. So these informations require protection.

(b) Top Secret – Information that need very high protection and unauthorized disclosure could severely damage national security e.g., vital defense plans.

(c) Confidential – Information about strength of armed forces and other technical information related to police/CBI etc. are confidential information. The disclosure of these information to an unauthorized person may damage national security.

(ii) Non-classified Information – The subcategories of non-classified information are –

(a) Confidential Business Information – Sales and marketing plans, new product plans etc. are confidential business information. If these informations get disclosed then it may give loss in business.

(b) Routine Business Information – The business information that can be shared inside or outside of the business time to time and do not require any special protection.

(c) Private Information – The credit card details, debit card details etc. are private information. These information can be associated with an individual.

(d) Personal Information – The informations such as e-mail ID, addresses, phone numbers, mobile numbers etc. are personal information. These informations belong to a private individual but can be shared with others for business or other purposes.

(e) Public Information – The information that is publically available or matter of public knowledge.

Q.26. Explain the types of identity theft.

Ans. Since the identity of someone is stolen for committing a crime. There are many types to which identity theft is related. Some of them are as follows –

(i) Financial Identity Theft – The US Secret Service has investigated 25 types of financial identity thefts in total. Bank fraud, credit card fraud, mail fraud etc. are financial identity thefts. When someone else's identifying details such as name, address, bank account details, etc. are used by fraudsters to commit fraud that is applicable on victim's finances e.g., new credit card accounts can be opened in the name of victim and the card charges up, payment is neglected, leaving the victim with bad credit history and large amount of debt. Sometimes the fraudsters are able to open a new bank account by completely taking over the victim's identity. He/she can purchase a vehicle, can get a mortgage loan etc. by using victim's identity.

To get recover from this crime expensive, time consuming and sometimes psychologically painful. A fraudster may be capable to spend thousands to lakhs of rupees, before the crime is detected, in victim's name.

(ii) Criminal Identity Theft – To commit a crime such as entering into a country, and any terrorist activity, by taking over someone else's identity, is known as criminal identity theft. Computer and cybercrimes, organized crime, drug trafficking, alien smuggling and money laundering can also be included in this crime/criminal activity.

The identity theft is always not for stealing money or to destroy victim's credit. When a fraudster uses victim's name upon arrest/during a criminal investigation. The fraudster may provide counterfeited information to law enforcement officer. What warrant has been issued in his/her name, the victim of criminal ID theft may not know this for a long time.

(iii) Identity Cloning – The frightened variation of all identity theft is identity cloning. The cloning of identity compromises the victim's life by actually living and working as victim, besides of stealing the personal information for financial gain or committing crimes in the victim's name. However cloner of ID may pay bills regularly, get engaged and even got married. It means that like victim's life, fraudster may live natural and usual life may be at a different location.

As much information as possible are obtained by an identity cloner. They will try to find all information related to the victim such as in which city or state the victim was born, in which street he/she lives, where he/she attended the school, how many members are there in his/her family etc.

(iv) Business Identity Theft – The information about the business/ organization privileged in nature and/or proprietary information which, if it is compromised through alteration, corruption, loss, misuse or unauthorized disclosure, could cause a big damage to the organization, is known as business sensitive information (BSI).

To steal business identity, Bust-out is a scheme that fraudsters use. In compare to individual's ID theft it is paid less importance. A space is rented by fraudster in the same building as victim's office. After that corporate credit cards are applied using victim's firm name. Since the company's name and address matches, the application passes credit check, but the cards are delivered to fraudster's mailbox. These cards are used by fraudster and destroyed before the victim comes to know that the firm's credit is badly damaged.

(v) Medical Identity Theft – Now-a-days, India has become famous for *medical tourism.* Because reasonable priced in medical services and good quality, India has made name so many tourist visit India every year with dual purpose – touring the country plus getting their medical problems attended to. The thousands of medical records of foreigners as well as locals are created in this process.

Healthcare facilities now are very different compared to how they were used before. When multiple agencies are connected over computer networks and Internet, these are great opportunities for protected health information (PHI).

Now the bulky paper records are changed to faster and easier file and trace electronic records by medical facility providers, even though the concept of medical ID theft is growing. The people who need the stolen information they buy it from fraudsters or fraudster can use it this information for other purposes.

If the victim's identity is successfully stolen by a fraudster and he receives the treatment, then this becomes the part of victim's permanent medical record.

(vi) Synthetic Identity Theft – In this theft, the fraudster takes some part of information from many victim's identity and combine them to generate a new ID, which is not of a specific person. But this can affect all the persons whose information is used. This is an advanced form of identity theft.

(vii) Child Identity Theft – The identity of child is theft by their parents to open bank accounts, credit card accounts or even to take out loans because their own credit history is too damaged or not sufficient. This theft is known as child identity theft.

Q.27. Describe the various techniques of identity theft.

Ans. The techniques of identity theft are given below –

(i) Traditional/Human-based Methods – In this technique there is no use of technology, and/or minimal use of technology. Following are subcategories of human based methods –

(a) Direct Access of Information – People who are very much trusted by the victim's such as peon, friends, relatives, roommates etc. can

obtain an authorized access to a business or residence to steal the required information.

(b) Dumpster Diving – Retrieving the documents by looking into the trash for information written on pieces of paper. In this the commercial or residential trashes are rummaged to find useful free items. It is also called binning, trashing, dumpstering.

(c) Wallet Theft – Pickpockets often work on a public place or in street to steal the wallets and sell the personal information received from wallet. Our wallet often contains adhar card, PAN card, driving license, credit/ debit card etc.

(d) Mail Theft and Rerouting – Since the mailbox has poor security mechanism, so it is easy to steal mails from it and all documents, which are freely available to the fraudster.

(e) Shoulder Surfing – Peoples who are standing in public facilities such as in cybercafes, near ATMs to keep watch over a person's shoulder while he/she logs into the system and grab personal information.

(f) Skimming – It is possible to install a mini equipment on a valid ATM, just as to imitate an ATM. Card informations are captured by this equipment and used to make duplicate cards. The PIN can be obtained by stealing the films of camera.

(g) Dishonest or Mistreated Employees – The personal files, salary information, bank information etc. can be accessed by an employee or partner, to gather all type of confidential information. The fraudster then can make sufficient damage by using these informations.

(h) Fake Telephone Calls – In this method the caller asks the victim to verify his/her account details immediately otherwise his/her bank account or ATM card will be suspended. This is very effective method of collecting information.

(ii) Computer-based Techniques – In these techniques the attackers make an attempt to exploit the vulnerabilities within existing processes and/or systems. The computer-based techniques of ID theft are –

(a) Backup Theft – In this method attackers also strike public facilities like transport areas, hotels, etc. as well as stealing equipment from private buildings. The stolen equipments or backups are carefully analyzed by them to recover the data.

(b) Hacking and Database Theft – The information systems are attempted to compromise with various tools, methods and techniques to get unauthorized access by criminals, besides the stealing of equipment.

(c) Phishing – In this method, the fishers try to get the user to disclose personal details such as credit card numbers, passwords, account information by covering the user to provide it necessarily.

(d) Pharming – In this method, the typo or matching domain names of the target are setup by attacker. Here the websites having the similar look and feel are installed.

(e) Redirectors – Here the users' network traffic is redirected to locations they did not intended to visit. The highest volume in traffic occurs with malicious code that simply modifies the victim's DNS server settings or the host files to redirect DNS lookups to a fraudlent DNS server.

Q.28. What is the cyberterrorism ? Discuss in detail. (R.G.P.V., Nov. 2018)

Ans. The term cyberterrorism was introduced by Barry collin in 1997, who was a senior research fellow at the institute for security and intelligence in california. It is like to be a controversial term. Related to deployment a very small definition was chosen by some authors from know terrorist organizations of disruption attacks against information systems for the primary purpose of creating alarm and panic. But this narrow definition made it difficult to identity any instance of cyberterrorism. Then Kevin G. Coleman of the Technolytics institue defined cyberterrorism as –

"The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives."

The term cyberterrorism has two words – cyber which is familiar to most of the peoples and terrorism which is less familiar. Since we can understand the term cyber but the term terrorism is difficult to define. The ambiguity in the definition brings in vagueness in action, as D. Denning pointed in his work saying that "An e-mail bomb may be considered as hacktivism by some and cyberterrorism by others". Everybody can understand the term cyberterrorism, either from the popular media or from the personal experience. The convergence of cybernetics and terrorism was defined as cyberterrorism by Barry Collin. The special agent for the FBI gave a definition in the same year.

"Cyberterrorism is the premediated, politically motivated attack against information, computer systems, computer programs and data which result in violence against noncombatant targets by sub national groups or clandestine agents.

Q.29. What is virtual crime ? Explain.

Ans. The word virtual crime has a part of problem within the word 'virtual', itself, which has become increasingly lacking of meaning. Sometimes virtual is used to refer to things that are practically the same in effect as the term modified and sometimes it simply refers to representations of things "created simulated or carried on by means of a computer or computer network."

Virtual crimes may be equated to cybercrimes by a narrower definition, defining cybercrime as "crimes committed by means of a computer or against the computer". Massively multiplayer online Game (MMOG) is an example of virtual crimes. We can only describe the virtual crime by MMOG. So we can say that virtual crimes are limited to only MMOG. MMOG is a video game, which is played and accessed by thousands of players with the conditions that Internet access and atleast one permanent virtual world is needed. There are many forms of MMOG some of them are –

(i) MMORPG – Massively Multiplayer Online Role-Playing Game.
(ii) MMORTS – Massively Multiplayer Online Real Time Strategy.
(iii) MMOFPS – Massively Multiplayer Online First Person Shooter.
(iv) MMOSG – Massively Multiplayer Online Social Game, etc.

The first multiplayer online game was introduced in 1987s and it become popular in 1990s. The most recent advancement in the scope of MMOG is second life in MMOSG. Now the authors of MMOG are calling it "3D virtual world" instead of "Game". Second life is a parallel virtual world with its inhabitants, who perform their own ideas and needs such as communication among them, meeting to new friends buying, studying, entertaining themselves in bars or cafes etc.

Now worldwide known companies like Dell, Adidas, Mazda, Vodafone, Philips etc. and hundreds of others have joined this virtual world for new product testing and for the support of real product sale. So this game is now only for fun but for other activities also.

The connection between real world and virtual world can be established on several levels. Few months ago there was a news that the second life has its first millionaire named Anshe Chung who was a avatar created by Ailin Graef and her husband.

They earned their first million by virtual real state trading. Although only Linden dollars can be paid in second life. Linden dollars can be purchased and sold for real money (US dollars) in LindenX exchange office or in exchange offices of third parties.

In second life, all rights are assigned to the authors of created world, like creating characters, clothing, scripting, objects and other design. So these possibilities give freedom for fraudlent acts and for infringements of intellectual property law. In 2007 six dealers who was offering their goods in second life field an action agaisnt another user for an illegal copy of digital wares.

In other MMOG types we can find that individuals are abusing the virtual environment with the intent to enrich themselves. Other examples like gold farming or virtual mugging among the well-known illegal practices can be included.

PERCEPTION OF CYBER CRIMINALS – HACKERS, INSURGENTS AND EXTREMIST GROUP ETC., WEB SERVERS HACKING, SESSION HIJACKING

Q.30. Write a short note on hackers.

Ans. The meaning of the word hacker has been changed over the years with the change of technology. In present, there are two opposite meanings of hackers. First one in computer enthusiast as an individual who enjoys exploring the details of computers and how to stretch their capabilities. Though most of the users prefer to learn only the minimum necessary. The second and opposite is a malicious or curious busybody who tries to discover information by poking around.

The people, who were highly knowledgeable about computing, were considered as hackers. They were considered computer experts who could do any wonder through programming on computer.

A process of gaining unauthorized access into a computer system for different purposes is known as hacking. Hacking has been used as a political or social demonstration during international crises.

Q.31. Explain different types of hackers.

Ans. Based on the phenomena of hacking there are several types of hackers. Some of them are as follows –

(i) Crackers – The attacker, who breaks security of a system is known as cracker. Crackers are professional security breakers and thieves. The term cracker was coined by purist hackers, who wanted to differentiate themselves from individuals with criminal motives whose sole purpose is to sneak through security systems. Purist hackers were worried that journalists were misusing the word hacker. They were worried that mass media has failed to differentiate computer enthusiasts and computer criminals.

Now the crackers are reforming by turning their hacking knowledge into legitimate use. They are forming enterprises to work with cyber security companies and sometimes law enforcement agencies to find and patch potential security breaches before their former counterparts can take advantage of them.

(ii) Hacktivists – The conscious hackers with a cause are hacktivists. They are originated from phreakers. Hacktivists carry out their activism in an electronic form in hope of highlighting what they consider noble causes such as institutional unethical or criminal actions and political and other causes. Hacktivists use several approaches to get the message across like real world. These approaches may be automated e-mail bomb, web de-facing, virtual sit-ins etc.

(iii) Cyberterrorists – Cyberterrorists can be divided into two categories based on their motives.

(a) Terrorists – The terrorist who are cyberterrorists have many motives, such as ranging from political, economic, religious, etc. Most often the techniques of their terror are through intimidation, coercion, or actual destruction of the target.

(b) Information Warfare Planners – Attacking a target by disrupting the target's essential services by electronically controlling and manipulating information across computer networks or destroying the information infrastructure to threaten the war planners.

Q.32. What are the different classes of hackers ? Discuss them in brief. ***(R.G.P.V., Dec. 2010, June 2011)***

Or

Write short note on classes of hacker. ***(R.G.P.V., Dec. 2013)***

Or

Discuss the classes of hackers. ***(R.G.P.V., Dec. 2016)***

Ans. There are many ways to classify those who break into computer systems, depending on which source you are reading. However, most lists of the types of hackers include the following –

(i) Black Hat Hackers – Black hats are the bad guys – the malicious hackers or crackers who use their skills for illegal or malicious purposes. Black hat hackers are motivated by greed or desire to cause harm. They target specific systems, write their own tools, and generally attempt to get in and out of a target system without being detected. Because they are very knowledgeable and their activities often undetectables black hat hackers are among the most dangerous.

(ii) White Hat Hackers – This group considers itself to be the ***good guys.*** Although white hat hackers may crack a system, they do not do it for personal gain. When they find a vulnerability in a network, they report it to the network owner, hardware vendor or software vendor, whichever is appropriate. They do not release information about the system vulnerability to the public until the vendor has had a chance to develop and release a fix for the problem. White hat hackers might also be hired by an organization to test a network's defenses.

White hat hackers are very knowledgeable about networking, programming, and existing vulnerabilities that have been found and fixed. They typically write their own cracking tools.

(iii) Grey Hat Hackers – Grey hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Both are powerful forces on the Internet, and both will remain permanently. And some individuals qualify for both categories. The existence of such individuals further clouds the division between these two groups of people.

(iv) Suicide Hackers – Hackers in this category perform their activities with little regard for the law or staying undetected. They seek to accomplish their goals at all costs and do not worry if they are caught. Their goals could include political, terrorist or other aims.

Q.33. Write short note on footprinting. ***(R.G.P.V., Dec. 2012)***

Ans. Footprinting is the first and most convenient way that hackers use to gather information about computer systems and the companies they belong to. The purpose of footprinting to learn as much as you can about a system, it's remote access capabilities, its ports and services, and the aspects of its *security.*

In order to perform a successful hack on a system, it is best to know as much as you can, if not everything, about that system. While there is nary a company in the world that is not aware of hackers, most companies are now hiring hackers to protect their systems. And since footprinting can be used to attack a system, it can also be used to protect it. If you can find anything out about a system, the company that owns that system, with the right personnel, can find out anything they want about you.

Footprinting is necessary for one basic reason – it gives you a picture of what the hacker sees. And if you know what the hacker sees, you know what potential security exposures you have in your environment. And when you know what exposures you have, you know how to prevent exploitation.

Hackers are very good at one thing – getting inside your head, and you do not even know it. They are systematic and methodical in gathering all pieces of information related to the technologies used in your environment. Without a sound methodology for performing this type of reconnaissance yourself, you are likely to miss key pieces of information related to a specific technology or organization – but trust me, the hacker won't.

Be forewarned, however, footprinting is often the most arduous task of trying to determine the security posture of an entity; and it tends to be the most boring for freshly minted security professionals eager to cut their teeth on some test hacking. However, footprinting is one of the most important steps and it must be performed accurately and in a controlled fashion.

Q.34. Explain the extremists and insurgents groups.

Ans. Extremists have redoubled their efforts to pursue their objectives (which are not based on truth or fact) of creating violence and instability

across the world, with terrorists. The year 2014 was worst year, in last 18 years, because 93 countries were experiencing an attack. Approx 32700 peoples were killed across the world in these attacks. The groups like ISIS (Islamic State of Iraq and Syria) and Al Qaeda were the main sources of the violence. These groups are more than just loose associations of radicalised fighters.

The threats will grow at rapid pace because in some regions/countries these terror organizations have sub-contracted their operations to mercenaries, criminals and warlords. Hence the vulnerability would be created by such global networks, even where the terror organizations do not have their footprints.

India is facing with multiple threats from religious and ideological, secessionist and saparatists organizations. The threat is from Islamic terrorists, left wing extremists (LWE), secessionist organization from the North-East and now even from communal forces. The challenges before the government is to protect the citizenship of country by preventing and denying recruitment of the youth into terror/insurgent organizations, keeping terrorists out of the society, denying their access to funds, weapons and safe havens, striping the terrorists from their roots and prevent networking between insurgent groups and various terror organizations.

In cyber terminology the insurgency is defined as *"An organized movement aimed at the disruption of cyber systems and through subversion and armed cyber conflict"*.

There may be different goals of cyber insurgency but the following conditions are necessary –

(i) Common entity or authority against whom, actions are directed, is must.

(ii) The tools of cyber insurrections and the systems to launch attacks against the entities are needed.

(iii) Cyber forces may be used by the cyber insurgents, against their targets.

The cyber security professionals learn from the records of irregular or low intensity warfare to better understand how to fight against this thread. This means that how can we modernize our strategies of cyber security.

The Internet has become a tool for radicalisation, recruitment, communication and training for terrorists and extremists. As a medium the decentralised nature of the Internet has made it difficult to governments to respond to threats emerging from it all over the world.

The terrorist groups are using social media as a way to violence. It is used for operations, ideation, indoctrination and recruitment. It targets people to inspire them to take action individually, making it hard for states to identify and track them.

Q.35. What do you mean by hacking of web servers ?

Ans. Since the term server is related to hardware and software so there are two meanings as hacking web servers. In hardware context – a web server is a computer, on which websites are hosted. In software context – a web server is a virtual program that runs on a computer to deliver the content, such as web pages and documents using the HTTP over the world wide web.

Any computer on the Internet containing website must have a web server program. A web server is used to provide various types of services, such as sending and receiving e-mails, downloading requests for a file and even more.

Therefore there are great chances of web server hacking. Web server hacking is a technique that completely relies on HTTP traffic to attack and penetrate web servers for defacement of websites.

There are following possible methods to hack web servers –

(i) Types of web server vulnerabilities

(ii) Web server defacement

(iii) IIS exploits.

(iv) Web server protection checklist.

The methods given above can be used to hack a web server as follows –

(i) Types of Web Server Vulnerabilities – A web server can be hacked by finding vulnerabilities in it. There are few common vulnerabilities discuss below –

(a) Misconfiguration – Generally Microsoft's IIS acts as a web server to use the default website. The persons who are using default website can access all the files in the default website folder. Similarly the users have permissions to execute full control of the file. Consequently, the default website is open to attack.

(b) Bugs – These includes operating system bugs, application bugs, or flows in the programming code.

(c) Default Installation – The default setting of a web browser software or operating system should be updated on a regular basis always and must not be left as default.

(ii) Web Server Defacement – A web server defacement or a website defacement means that a hacker attacks on a website and changes the visual appearance of website. Mainly web server listens to port 80 (HTTP) and port 443 (TCP). Therefore these port needs to be open for passing traffic between the web server and the client.

(iii) IIS Exploits – Windows IIS is one of the popular web server products. Therefore, web servers that run IIS, have more probability to be

attacked. Some common IIS attacks are given below –

(a) Directory Traversal – These attacks mainly depend on assumptions, because within the windows file system the web clients are limited to specific directories within the windows file system. One of the common directories is root directory. The directory traversal attacks can be applied on this directory. Most of the clients access this directory.

The root directory stores the home page of a website, index or other documents for the webserver. A roof directory includes subdirectories. These sub-directories store other types of file such as a scripting file.

(b) Source Disclosure – This type of attack accesses the source code of application running on a web server and with the help of this source code, a hacker identifies the history of the application such as application type, programming language, and much more information.

(c) Buffer Overflow – In this attack a large amount of data a large amount of data is sent to a web server. Therefore the server needs capacity to handle the data. In such cases the web server is unable to handle the data. So buffer overflow takes place.

(iv) Webserver Protection Checklist – When we need to protect our web server, we can use web server protection checklist. This checklist contain some parameters by using which hackers can attack on the web server.

Q.36. What do you mean by session hijacking ? (R.G.P.V., Nov. 2019)

Ans. Session layer protocols maintain state through a session identifier, and the identifiers are usually valid for an extended period. If the session identifier is not encoded, then an attacker may acquire the session identifier and hijack the session. This is a common style of network attack, and referred to as session hijacking.

Web cookies readily lend themselves to session hijacking. Many computer viruses, like Sasser and Berbew, harvest Web cookies from infected hosts. These cookies store active session information, allowing an attacker to effectively hijack a session. For example, some variants of Agobot looked for Web cookies associated which Bank of America and sent them to a remote system managed by the attacker. Using the stolen cookie, the attacker could access the Bank of America account without needing login credentials.

To mitigate attacks from stolen sessions, cookies should be disabled or removed when the browser closes. Cookies may be cryptographically linked to a specific network address. Since network addresses are difficult to forge outside of the local network, hijacking becomes much more difficult. Furthermore, Web servers configure Web cookies with specific lifetimes; after expiration, the cookie is no longer valid. These servers can protect their customers by assigning cookies with short lifetimes. Unless the cookie is stolen and used immediately, the expired session has little value to an attacker.

Kerberos uses many of these mitigation steps. Each ticket has a limited duration. Before the ticket expires, the client "renews" the ticket by requesting a new session identifier. Kerberos tickets are associated with client-specific information (client certificate, session key, etc.) and are cryptographically protected. Assuming an attacker can get past the encryption and impersonate the client, the limited session duration restricts the window of opportunity for a viable exploit.

Q.37. How does session hijacking work ?

Ans. As we know, the http communication uses many TCP connections and so that the server needs a method to recognize every user's connections. The most used method is authentication process and then the server sends a token to the client browser. This token is composed of a set of variable width and it could be used in different ways, like in the URL, in the header of http requisition as a cookie, in other part of the header of the http request or in the body of the http requisition. The attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the web server. The compromisation of a session token can be occurred in different ways, two of them are as follows –

(i) Session Sniffing – We know that, there is a string called tokens, is the session id of a valid session. The attackers firstly try to find this session id. The attackers uses a sniffer to get this session id. When the session id is captured, the attacker uses this session id to gain unauthorized access to the web server.

(ii) The Cross-site Script Attack – The way, to get the session id with the help of running a malicious code or script from the client side, is cross-site script attack. In this attack, the malicious script also known as malicious payloads are executed into a legitimate website or web application by the attacker. In this attack the victim is not targetted directly by the attacker, but the attacker could exploit a vulnerability in a website that the victim would visit and use the website to deliver malicious script to the victim's browser.

Q.38. How can we prevent session hijacking ?

Ans. As we know that the session id is stolen by installing a malicious code on the client website and then the cookies are stolen. The best approach to prevent session hijacking, is that the protection should be enabled from the client side. Taking preventive measures on the client side for session hijacking

is highly recommended. The users should have efficient antivirus, anti-malware softwares and should keep the softwares up-to-date.

There is a technique that uses engines which fingerprints all requests of a session. Beside the tracking IP address and SSL session id, the engines also track the http headers. Each change in the header adds penalty points to the session and the session gets terminated as soon as the points exceeds a certain limit. This limit can be configured. This is effective because when intrusion occurs. It will have a different http header order.

These are the recommended preventive measures to be taken from both the client and server sides, in order to prevent the session hijacking attack.

■■

UNIT 3

CYBERCRIME AND CRIMINAL JUSTICE – CONCEPT OF CYBERCRIME AND THE IT ACT 2000, HACKING, TEENAGE WEB VANDALS, CYBER FRAUD AND CHEATING, DEFAMATION, HARASSMENT AND E-MAIL ABUSE

Q.1. Define the concept of cybercrime and the Indian IT act 2000.

Ans. After the United Nation General Assembly Resolution A/RES/51/162 IT Act 2000 was enacted by taking the Model Law on Electronic Commerce taken by the United Nations Commission on International Trade Law.

The term cybercrime is not defined in the Indian IT Act 2000. Generally there are two definitions of cybercrime. In first definition it can be defined that "cybercrime contains only those crimes which are included in IT Act 2000". This definition is only limited to tampering with computer source code, hacking and cyber pornography. Other cyber related crime such as cyberdefamation, e-mail spoofing, cyberfraud etc. would not be treated as cybercrime.

The second definition can be given as – "A crime which is committed or omitted, with the help of or through or connected with Internet, and prohibited by law and if the punishment for which by penalties or imprisonment is provided then it will be called cybercrime".

This definition is also not covering all the crimes in the Indian IT Act 2000. For example – A person is threatening the other on Internet and he commit sucide then that person will be charged the offence of criminal intimidation under section 506 of IPC, 1860. He will not be charged under Indian IT Act 2000. Since, there are few cybercrimes which are included in IT Act 2000 and there are many crimes other than crimes included in IT Act 2000, in cyberspace which are given in IPC 1860.

The Indian IT Act was enacted in 2000. The purpose of Indian IT Act 2000 was to make changes in the Indian Penal Code (IPC), the Indian Evidence Act 1872. The Banker's Books Evidence Act 1891, the Reserve Bank of India

Act 1934. The section 58B about penalties was included in the Reserve Bank of India Act. Some important changes in the IT Act 2000 were introduced to accommodate the current cybercrime scenario.

Q.2. What is IT Act 2000 ? Write the silent features of IT Act 2000. ***(R.G.P.V., Nov. 2018)***

Ans. **IT Act 2000** – Refer to Q.1.

Features of IT Act 2000 – Features of Indian IT Act 2000 are as follows–

(i) An e-mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. IT Act 2000 change this scenario by legal recognition of the electronic format.

(ii) The ITA 2000 has provided legal infrastructure for companies in corporate sector to carry out e-commerce transactions.

(iii) The concept of digital signature is provided for corporates to carry out their transactions online. The digital signatures are legally valid and sanctioned under the ITA 2000.

(iv) Now, the companies are storing the information on their respective computer system, apart from maintaining a backup. It became possible for corporate to have a statutory remedy if anyone breaks into their computer systems and causes damages or copies data, under ITA 2000. The remedy provided by the ITA 2000 is in the form of monetary damages, by the form of compensation, upto ₹10,000,000.

(v) Various cybercrimes were defined in ITA 2000. Before the cyberlaw came into the effect, the corporate were helpless as there was no legal redress for such issues.

Q.3. What are the limitations of IT Act 2000 ?

Ans. The limitations of IT Act 2000 are as follows –

(i) The issues related to domain names are not included in ITA 2000. Since e-commerce is based on system of domains and domain names have not been defined in the IT Act 2000. The rights and liabilities of domain name holders are not included in the law.

(ii) The issues concerning the protection of Intellectual Property Rights (IPR) in the context of the online environment, are not dealt in ITA 2000. The issues related to online copyrights, trademarks and patents etc. are not covered in this law.

(iii) There are many new forms and manifestations of cybercrimes as far as the cyberlaws are getting developed. The offenses defined in the ITA 2000 are by no means exhaustive. It does not cover various types of cybercrimes such as Internet Time Theft, cyberdefamation, cyberfraud, cyberharassment, misuse of credit card, cyberstalking etc.

(iv) The ITA 2000 has not tackled vital issues pertaining to e-commerce sphere like privacy and content regulation to name a few.

(v) The applicability of IT Act to negotiable instruments is avoided because the IT Act is not explicit about regulation of electronic payments. The IT Act stays silent over the regulation of electronic payments gateway and rather segregates the negotiable instruments from the applicability of IT Act. This may have major effect on the growth of e-commerce.

(vi) The antitrust issues are not included in the IT Act.

(vii) The IT Act 2000 does not lay down parameters for its implementation, so this is the most serious concern related to the Indian cyberlaws. Also when Internet penetration in India is extremely low and government and police officials are not very computer savvy, the new Indian cyberlaw raises more questions than it answers.

(viii) There may be a conflict of jurisdiction and IT Act 2000.

Q.4. What is the need of cyberlaw in India ?

Ans. A framework that is created to give legal recognition to all risks arising out of the usage of computers, computer systems, or computer networks. There are many aspects such as data protection and privacy, freedom of expression and crimes committed using computers comes under the cyberlaw. The first cyberlaw passed by Indian Parliament was the IT Act 2000, of which aim was to provide legal infrastructure for E-commerce in India. The ITA 2000 was approved by the President of India and now it has become the law of the land in India. To regulated Internet-based computer-related transactions in India, the Government of India felt the need to pass a relevant cyberlaw. It was mentioned that the ITA 2000 was an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, referred to as e-commerce, while it was introduced.

The reasons to pass the IT Act 2000 in India are as follows –

(i) Although all possible situations and cases that have occurred or might take place in future are covered in a very well-defined legal system in India, when it comes to newly developed Internet technology the country lacks in many aspects. Because of this increasing use of Internet it was necessary to fill this gap with suitable law.

(ii) Since Internet is most dominating source of carrying out business today, therefore, there was a need to have some legal recognition to the Internet.

(iii) A new concept called cyberterrorism came into the effect, with the growth of the Internet. Cyberterrorism includes the use of disruptive

activities with the intention to further social, ideological, religious etc. or similar objectives in the world of cyberspace. It was about committing an old offence but in an innovative way.

Considering all these factors, the Information Technology Bill was passed on 17 May 2000 by Indian Parliament. It was called IT Act 2000.

Q.5. Why we need cyber security explain ? ***(R.G.P.V., Nov. 2019)***

Ans. Its being protected by internet-connected systems, including hardware, software and data, from cyber attacks. In a computing context, security comprises cyber security and physical security both are used by enterprises to safe against unauthorized access to data centre and other computerized systems. The security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.

The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats are as follows –

Cyber Terrorism – It is the innovative use of information technology by terrorist groups to further their political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.

Cyber Warfare – It involves nation-states using information technology to go through something another nation's networks to cause damage. In the U.S. and many other people live in a society, cyber warfare has been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers who are well-trained in use of benefit the quality of details computer networks, and operate under the favourable and support of nation-states. Rather than closing a target's key networks, a cyber-warfare attack may forced to put into a situation into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.

Cyber Spionage – It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malware.

Q.6. What is hacking ? ***(R.G.P.V., Dec. 2015)***

Or

Write short note on hacking. ***(R.G.P.V., June 2012)***

Ans. The term ***hacking*** used to mean expert writing and modification of computer programs. Hackers were considered people who were highly knowledgeable about computing. They were considered computer experts who could make the computer do all the wonders through programming. Today, however, hacking refers to a process of gaining unauthorized access into a computer system for a variety of purposes including stealing of and altering of data and electronic demonstrations. For some time now, hacking as a political or social demonstration, has been used during international crises. During a crisis period, hacking attacks and other Internet security breaches usually spike, in part because of sentiments over the crisis.

Q.7. Write short note on hacking tools. ***(R.G.P.V., Dec. 2003, 2011)***

Ans. Attackers use several tools to gain access to secure systems. Some of those tools are –

(i) Password Guessing – Because access to most programs depends on password authentication protocol (PAP) there would-be attacker attempts to guess both user name and password. User name is usually simple because it often is also used as an e-mail ID. The determination of the password is a calculated guess. Fig. 3.1 shows the PAP process.

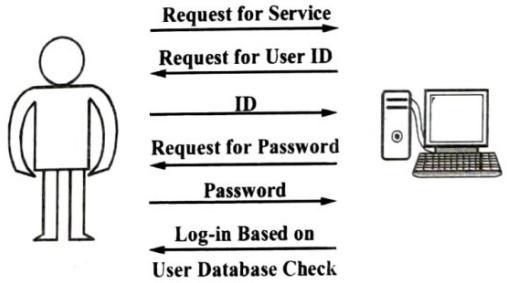


Fig. 3.1 Password Authentication Protocol

Therefore passwords must be designed and controlled to make their guessing a very complex proposition.

(ii) External Programs – Several remote programs are used to attempt to capture and control the operation of a computer and access, read, manipulate, or delete data. Table 3.1 lists a few examples with a definition of their legitimate purpose.

Table 3.1 External Programs

Telnet	A virtual terminal program that permits a remote device to attach itself to a local computer in the form of a terminal and is used by systems people to update and manipulate files.
Network management software	Tools designed to access remote systems resources for management purposes.
Port mappers	Used by administrators to determine users and processes operating certain shared systems.
Database replication services	Software tools used to transfer record updates to server databases

(iii) Malicious Programs – Fig. 3.2 shows an overall taxonomy of software threats, or malicious programs. These threats can be divided into two categories – those that need a host program, and those that are independent. The former are essentially fragments of programs that cannot exist independently of some actual application program, utility, or system program. The latter are self-contained programs that can be scheduled and run by the operating system.

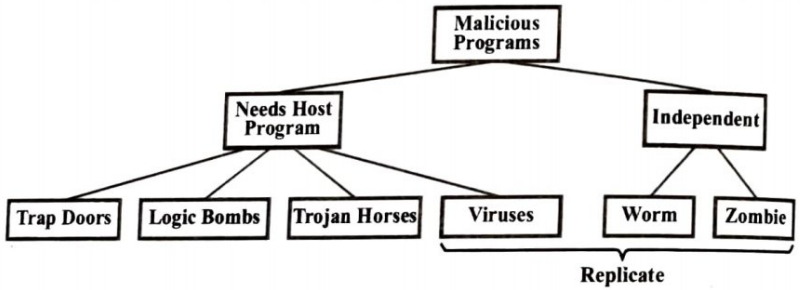


Fig 3.2 Taxonomy of Malicious Programs

Q.8. What do you mean by the term Teenage Web Vandals ?

Ans. Security experts also call the Teenage Web Vandals as – Packet Monkeys, Script Kiddies and Ankle-Biters. These are the teenage gangs, who love to play real games in virtual world. Various opportunities, which were unimaginable before, were thrown in 1990s by the Internet and information technology.

Some examples of billionaires and super achievers are – Sabir Bhatia (founder of Hotmail), Jerry Yang (founder of Yahoo), Marc Anderson (founder of Netscape) etc., who became billionaires below the age of 35 years. But now to become billionaire and fame nobody have to wait till 35 years, because of

power and attraction of IT. But this attraction is also giving birth to teenage cybercriminals.

Either web pages are defaced or remarks are tagged on websites by most of these teenage web vandals. Now the cybercrime has become fashionable and favourite of netizens in India.

Even the web defacement and tagging of websites are harmless or may be annoying, but there is a fear creating in the Internet community, this fear has driven high cost of security, and there many doubts about future of e-commerce.

The motivating factors and causes of teenage web vandals are as follows–

(i) They want to be famous and publicity all over the world using Internet.

(ii) Excitement of achievement and greatness by doing something different.

(iii) There is no fear of the law and its enforcement due to anonymity provided by the system of the Internet.

(iv) They do not know the bad effects of the act of defacing or hacking. They think that, there is no loss caused by their acts.

(v) By doing this, they are claiming that they have a good knowledge of computer programming and Internet.

(vi) The knowledge, which is not in right direction of Internet and computer programming.

(vii) The resources are cheapest and easily available to commit hacking and defacement of websites.

Q.9. Discuss the term cyber fraud and cheating.

Ans. The frauds which are constituted on the Internet are known as cyber fraud. About one-third of all cybercrimes is constituted in cyber frauds. Cyber frauds are increasing day by day. Cyber frauds are increasing with the growth of e-commerce because it's profitability is in unleashing the e-commerce. Victims of cyber fraud do not disclose the case because of fear of loss of public trust, image, business etc. Some cases of cyber frauds and cheating include misuse of credit cards by hacking the password, bogus investment illegal transferring the funds etc.

The term is not included in the IT Act 2000, so we will have to follow other laws of Indian Penal Code 1860, or Indian Contract Act 1872 etc. The acts given below are the meaning of fraud.

(i) The suggestion which is not true.

(ii) Promising somebody and intention of his/her is not to fulfil it.

(iii) The omissions or acts which are declared by the law are fraudulent.

In the law of contract this definition of fraud is applied to contractual or civil relations between parties and has no applicability to criminal law. Hence for the purpose of criminal law, the term cyber fraud would be a improper or in appropriate and instead of this the term cyber cheating would be more appropriate in India. The term cyber fraud in India can be used for only civil laws and law of contract, for claiming damages and compensation.

For the acts of cyber cheating not only the punishment under the criminal law but also the compensations for damages under civil laws are included. There is no definition or offence of fraud in the Indian Penal Code (IPC), even many other contents which contain the ingredient of fraudlent actions are there.

The ingredients of cheating are as follows –

(i) When a person make a false representation and to which he/she knows that it is false, is known as cheating.

(ii) Deceiving a person by making a false representation with him/her, with the intention of dishonestly, is known as cheating.

(iii) The deceived person is induced to deliver any property or to do or omit to do something.

The punishment for cheating a person/firm is imprisonment which may be extended to one year or fine or both.

Q.10. Describe various offences of fraud and cheating in the Indian Penal Code which are similar to cyberfraud.

Ans. There are some provisions in the Indian Penal code which are similar to cyberfraud. These offences with IPC section and punishment are given in table 3.2.

Table 3.2

S.No.	Section in IPC	Offence/Provision	Punishment
(i)	403	Dishonest misappropriation of property.	Imprisonment for a term which may be extended to two years or with fine or both.
(ii)	405, 406	Criminal breach of trust.	Imprisonment for a term which may be extended to three years, or with fine or both.
(iii)	408	Criminal breach of trust by clerk or servant.	Imprisonment for a term which may be extended to seven years and fine.
(iv)	409	Criminal breach of trust by a public servant or by a banker, merchant, factor, broker, attorney or agent.	Imprisonment for life, or with imprisonment for a term which may be extended to ten years and fine.
(v)	463/465	Forgery	Imprisonment for a term which may be extended to two years, or with fine or both.
(vi)	464	Acts amounting to making a false document.	–
(vii)	466	Forgery of records of Court or of public registrar.	Imprisonment for a term which may be extended to seven years and fine.
(viii)	468	Forgery for the purpose of cheating.	Imprisonment for a term which may be extended to seven years and fine.
(ix)	469	Forgery for the purpose of harming reputation.	Imprisonment upto three years and fine.
(x)	470	When a false document is a forged document.	–
(xi)	471	Using a forged document as genuine.	Imprisonment for a term which may be extended to two years, or with fine, or both.
(xii)	476	Counterfeiting device or mark used for authenticating documents other than those described under section 467, or possessing counterfeit marked material.	Imprisonment for a term which may be extended to seven years and fine.
(xiii)	477	Fraudlent cancellation, destruction, etc. of a valuable security etc.	Imprisonment for life or imprisonment for a term which may be extended to seven years and fine.
(xiv)	477A	Falsification of accounts.	Imprisonment for a term which may be extended to seven years or with fine or both.
(xv)	481	Acts amounting to using a false property mark.	–

(xvi)	482	Punishment for using a false property mark.	Imprisonment for a term which may be extended to one year or with fine or both.
(xvii)	483	Counterfeiting a property mark used by another.	Imprisonment for a term which may be extended to two years or with fine or both.
(xviii)	484	Counterfeiting a mark used by a public servant.	Imprisonment upto three years and fine.
(xix)	485	Making or possession of any instrument for counterfeiting a property mark.	Imprisonment for a term which may be extended upto three years or with fine or both.
(xx)	489	Tampering with property mark with the intention to cause injury.	Imprisonment for a term which may be extended to one year or with fine or both.

Q.11. What kind of statements are not considered as offence of defamation?

Ans. Statements which fall under the following ten exceptions are not considered as offence of defamation –

(i) If a statement is good for public and is true in concern of a person. It means that a statement that is true but harms the reputation is defamatory until and unless it is for the good of public.

(ii) When the functions of public servant are discharged then the opinion regarding the conduct by him in good faith, or regarding his character only like his character appears in that conduct.

(iii) The report or result of the proceedings of the court of justice, published.

(iv) When a person touches a question then the opinion in good faith regarding the conduct of him/her.

(v) The advantage of any case, civil or criminal, which has been decided by the court of justice, or regarding the conduct of a person as a party, witness or agent, in any such case, it is good for public.

(vi) The advantage of any performance, submitted to the public by author for judgement, or regarding the character of another unless his character appears in such performance, if it is good for public.

(vii) Passing any censure on the conduct of that other in matters by a person having authority over another in good faith.

(viii)Statements against any person to any of those who have lawful authority over that person with respect to the subject matter of the accusation made in good faith.

(ix) Statements, made in good faith for the protection of the interest of the person making it, on the character of another.

(x) A caution, conveyed by a person against another which is intended for the good of the person to whom it is conveyed, in good faith.

The law of defamation, attempt to balance the democratic freedom of speech and expression for public good, by providing above given exceptions.

Q.12. What is e-mail abusing ? How can the e-mail abusing be reduced ?

Ans. Unsolicited e-mail, which is also known as spam, is an increasing problem in the world. Our valuable time is robbed by e-mail spam. Network resources are consumed and storage space on our servers are used by e-mail spams.

To deal with e-mail spam, it is best not to reply to a spam message for any reason, this validates our e-mail address and will be resulted in more spams. When we are publishing web pages, we should use HTML sequence @ in place of the @ symbol in e-mail addresses to fool e-mail harvesters. The spam messages should be copied to UIS e-mail abuse (or emailabuse@uis.edu). We will block any incoming messages with recurring detectable and traceable origins. To copy e-mail to the UIS e-mail abuse mailbox. The offending e-mail message must be copied and not forwarded to preserve Internet headers. These headers allow us to trace the route. Steps to copy the e-mail message to UIS are as follows –

(i) In MS outlook left click on the e-mail message so that it is highlighted.
(ii) Click on edit on outlook menu bar.
(iii) Click on copy.
(iv) Now open a new mail message.
(v) Type UIS e-mail abuse or emailabuse@uis.edu in the to field.
(vi) Type e-mail abuse in the subject field.
(vii) Now click in the message area of the new message.
(viii) Now click on edit on the outlook menu bar.
(ix) Now click on paste.
(x) Click send.
(xi) Now use the delete key.
(xii) Use the junk and adult content filters in outlook (available under tools, organize).

A number of methods are used by criminals of e-mail spam, which make it very difficult for network and e-mail administrators to block their messages. The criminals often send their messages from a borrowed e-mail address, i.e. sending the message as someone else. Then they will change that address continuously so as to prevent their messages from being blocked. Spammers can spoof an e-mail address so as to make it appear to have originated from a legitimate website, google.com or hotmail.com. Spammers often relay their messages through three or four e-mail servers to make tracing messages back to the source difficult.

Q.13. What is harassment ?

Ans. Harassment through Internet has been spread everywhere. To make a person disturbed by making a lot of call or sending e-mails asking for contacts of call'girls, or some pornographic material or such other things that the person is not related to, is known as harassment. Harassment may be a major cyber-crime in near future. The problem of harassment is not restricted only to film stars and famous people even ordinary users of the Internet are using this medium for harassing their enemies.

OTHER IT ACT OFFENCES, MONETARY PENALTIES, JURISDICTION AND CYBERCRIMES, NATURE OF CRIMINALITY, STRATEGIES TO TACKLE CYBERCRIME AND TRENDS

Q.14. Explain the IT Act offences other than cyber crimes like hacking, teenage web vandals, cyberfraud and cheating etc.

Ans. There are certain other offences besides the cybercrime we have discussed, in the IT Act 2000. When the source code of computer which is used for a computer, computer network, computer program or computer system is altered or destroyed intentionally by a person, even the computer source code is required to be kept or maintained by law for the time being in force, then this is said, the offence of tampering with computer source documents.

This offence is punishable under section 66 of IT Act 2000 with the imprisonment for a term which may be extended upto three years or with fine which may be extended upto ₹ 2 Lakh or both. If the person fails to comply with the order of the Controller of Certifying Authorities, is punishable under section 68 of IT Act 2000, with imprisonment for a term not exceeding three years or with a fine upto ₹ 2 Lakh or both.

The controller of certifying authorities may direct any of the government to intercept any information transmitted through any computer, if he is satisfied that it is necessary in respect to integrity and sovereignty of India. Every user or incharge of computer will have to provide all facilities and help to decrypt the information. If anyone denies to assist the agency then he/she shall be punishable under section 69 of the IT Act 2000, with imprisonment for a term which may be extended upto 7 years.

A person who breaks the confidentiality and privacy, shall be liable for punishment, with imprisonment for a term which may be extended upto two years, or with fine which may be extended to ₹ 1 Lakh or both, under section 72 of IT Act 2000.

If a digital signature certificate is issued with the knowledge that issuing authority listed in the certificate has not issued it or the certificate has been revoked, then he/she shall be liable for a punishment under section 73 of IT Act 2000 with imprisonment for a term which may be extended upto years, or with fine upto ₹ 1 Lakh or both.

Q.15. What are monetary penalties ? When a criminal shall be liable to pay monetary penalties ?

Ans. When a criminal is punished to pay damages by only penalties for the offences instead of imprisonment, then these penalties are known as monetary penalties. There are many contraventions for which a person would be liable to pay damages by the penalties for non-compliance of certain requirements. If a person perform any or more of the following acts on computer, without the permission of owner or in-charge of a computer, then he/she shall be liable to pay damages by way of compensation not exceeding ₹ 1 Crore to the person affected, i.e. the victim –

(i) He/she accesses a computer, computer system or network for which he/she is not authorized.

(ii) Any data or copies of data extracted, or computer database or information from computer, or computer system or network is downloaded.

(iii) Computer viruses on any computer, or computer system or network are introduced.

(iv) Any computer or computer system or computer network disrupted.

(v) Any computer or computer system or network, data, computer database or any other program residing in such computer are damaged by the person.

(vi) Any authorized person denied to access the computer, computer system or computer network by him/her.

(vii) Facilitating access to a computer or computer system or network by providing assistance to any other person.

It is clear that infringements punishable with imprisonment are triable by criminal courts, whereas the infringements punishable with penalty or compensations have been left for adjudication by an adjudicating officer. For the purpose of adjudication of infringements for which compensation or penalties are provided, an adjudicating authority has been created separately. Any officer who is equivalent or above the rank of director to the Government of India or of State Government, shall be appointed by the Central Government.

Q.16. What is the meaning of the term jurisdiction ?

Ans. It is stated in the IT Act 2000, that an offence whether it is committed in India or outside of India by any person irrespective of his nationality would also be punishable unless or otherwise provided in the act. Though it is clear that the act shall be applicable to the offence committed outside India by any person, and if the offence committed involves a computer, computer system or computer network located in India.

The words "act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India" are very significant to determine jurisdiction of the IT Act over acts committed outside India. We have to prove that an act involve a computer or computer system or computer network is located in India, for the offence which is committed outside India, under the IT Act for assuming jurisdiction.

e.g., a website is created any where in the world contains pornographic materials. It will not provide IT Act jurisdiction to question the site unless the creation or running of the site involves any computer or computer system or computer network located in India. But if the website uses a server or computer network in India the IT Act would assume jurisdiction to question the website under section 67 of the IT Act.

Another example is that any computer or computer network is hacked by a person any where in the world, will explain the jurisdiction of the IT Act in India, to punish the accused the section 66 of the IT Act would be charged, because the his/her act involve a computer in India.

Q.17. What is the basic legal principle of jurisdiction under criminal procedure code ?

Ans. The basic legal principle of jurisdiction under the criminal procedure code, 1973 is that the offences which are committed would be tried and inquired within the courts whose local jurisdiction it was committed. These principles will be applied for determining jurisdiction in investigation by the police as well as in trial by courts. Whether an offence is committed in more than one places or party committed in more than one places or party committed in one place and partly in another place or it is continuously and continued to be committed in more than one places or the offence consist of several acts done in different areas, then it may be inquired or tried by the court having jurisdiction over either of such areas. On the other hand in the acts where it is uncertain that where the offences was committed, it would also be inquired or tried in the court having jurisdiction over either of such areas of uncertainty.

In other case where an act is an offence by any reason, which has been done, the offence may be inquired or tried into the court of which local jurisdiction the act has been done.

e.g., in the case of cyberdefamation either of the courts, i.e. of the place where the defamatory letter was e-mailed or place where it was received, if different, will be inquired or tried in court of same jurisdiction.

There are some certain offences which would be inquired or in tried in certain places.

e.g., an offence of criminal misappropriation or of criminal breach of trust may be inquired into or tried by the court within whose local jurisdiction the offence was committed.

Q.18. Describe the nature/characteristics of cybercrime.

Ans. The characteristics of cybercrime are as follows –

(i) Since cybercrimes are committed through technology, therefore the cyber criminal who have deep knowledge of the Internet and computer are technocrats.

(ii) Cybercrimes are very efficient because they take no more time in operating and affecting. The cyber criminal may hack a website or play cyberfrauds within a few seconds or minutes.

(iii) There are no geographical boundaries, limitations or distances in cybercrime. The computers can be hacked in India by the cyber criminal who are at any corner of the world.

(iv) The cyber criminals are almost invisible because cybercrimes take place in cyberspace. All the components of cyber criminality (from preparation to execution), take place in cyber world except the cyber criminal physically being outside the cyberspace. Since the cyber criminals are everywhere, so the risk factor in cyber criminality is very less in compare to traditional crimes.

(v) The websites can be destroyed, which were created and maintained with huge investments, or confidential websites can be hacked such as defence system of a country by committing cybercrime. So cybercrime can cause harm and injury which cannot be imagined.

(vi) Cyber criminals have the capacity to affect several countries at the same time, which are different from the place of operation of them, because of invisibility of cybercriminality.

(vii) The collection of evidences of cybercrime and proving them in the court of law is very difficult.

(viii) The tools to commit cybercrime can be easily and freely available in CDs in the market at very minimal charges, so cybercrimes are easy to commit.

Q.19. What are the different strategies to tackle cybercrime ?

Ans. Various strategies to tackle cybercrimes are as follows –

(i) The law enforcement agencies should be trained in the complicacies of technology, so they can effectively and property conduct their investigations. An investigator should be atleast a half IT engineer to be a competent investigator of cybercrime. To detect cybercrimes, technical tools such as trace and trap devices must be used by the investigator besides his/her technical knowledge.

(ii) The law enforcement agencies of different countries should be in cooperation because there is a tendency of jumping geographical borders.

(iii) To bring the cybercriminals for trial across borders, the effective laws of extradition and their implementations are must.

(iv) Encryption and other security technologies should be used to protect against cybercrime.

(v) It is the responsibility of the IT companies to protect it's own systems and networks by using technologies which are secured. The IT companies should not depend on the low enforcement agencies to track cybercriminals, because it is very difficult, since there is anonymity provided by the Internet.

(vi) The research and development of new security technologies must be facilitated and encouraged by the government. To support research and development and to facilitate education related to counter cybercrime, there should be a funding from government.

(vii) In the IT industry, the victim's are not reporting most of the cybercrimes, because of fear of losing the confidence of customers. Name & fame and the loss of business. Every victim should report the crime to low enforcement agencies. To deal with cybercrime more effectively the information about cybercrime, so as to understand it's various forms and ways, must be shared by private sectors.

(viii) One solution to fight against cybercrime is the easy identification of netizens. All the contents and interactions on the Internet should be censored, it is not recommended.

Q.20. Explain intellectual property right with suitable example.
(R.G.P.V., Nov. 2019)

Ans. The concept of intellectual property can be traced back to the Byzantine empire where monopolies were granted. For instance in greece a one year monopoly was given to cooks to exploit their recipes. A statutory legislation in the senate of venice provided exclusive privileges to people who invented any machine or process to speed up silk making. Thus, from intellectual property being totally alien to the nomadic community came an era where every new idea was given protection under the category of intellectual property rights. Copyright is known as one of the types of intellectual properties. Before going into details of the copyright and related issues in cyberspace, we need to know the concept of intellectual property and its importance. To go home is to enter a place built and filled with human creativity and invention. From a carpet to a sofa, from the washing machine, the refrigerator and the telephone, to the music, the books, the paintings, family photographs, everything which we live is a product of human creativity. These things are creations of the human mind and hence called intellectual property. Today the internet is not only used for educational purposes but also for business.

Intellectual property can be categorized into two categories i.e. industrial property and copyright. Industrial property deals with patents, trademarks, geographical indications, designs and semiconductors layout design. On the other hand copyright covers literary, dramatic, artistic, musical, cinematographic films and sound recording etc. The primary legislations regulating intellectual property in India are – The patents Act 1970, the trade marks Act 1999, the geographical indications of goods (registration and protection) Act 1999, the design Act 2000, the semiconductor integrated circuits layout design Act 2000 and the copyright Act 1957.

Q.21. Explain the term copyright act and patent law. (R.G.P.V., Nov. 2019)

Ans. **Copyright Act** – Copyright law protects original works of authorship that are fixed in a tangible medium of expression. Works of authorship include the following categories – literary works (including computer programs); musical works (including the accompanying words); dramatic works (including accompanying music); pantomimes and choreographic works; pictorial, graphic, and sculptural works; motion pictures and other audiovisual works; sound recordings; and architectural works.

The basic elements of a copyright are expression and originality. The originality requirement is met if the work is independently created by an author and not copied from others. Further, originality does not require novelty. Accordingly, a work will not be denied copyright protection merely because it is similar to a work previously produced by someone else and, therefore, not novel. An author or creator, however, is entitled to a copyright only in the expression of a work and not in the idea underlying the work. Consequently, copyright does not extend to an idea or fact.

For a work to be eligible for copyright protection, it must be "fixed in any tangible medium of expression, now known or later developed, from which [it] can be perceived, reproduced, or otherwise communicate[ed], either directly or with the aid of a machine or a device. A work is fixed in a tangible medium of expression "when its embodiment in a copy or phono record, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work, more than transitory duration.

A copyright owner's right to reproduce his or her work is an important aspect of the exclusive rights afforded by copyright law. At the same time, it allows the owner to preclude all others from making copies of the work. Copies, as defined in the copyright act, are material objects in which a work is fixed "by any method now known or later developed." Accordingly, an Internet user that makes an unauthorized copy of a copyrighted work is likely to be violating the copyright owner's rights.

A copyright owner also has the exclusive right to incorporate the work into derivative works and to exclude others from creating works based on his or her other work. The right of distribution assures the copyright owner of his

or her right to the first distribution of the work. Thereafter, however, the first sale doctrine – which attempts to strike a balance between providing the copyright owner with the benefits of the copyright protection and permitting unimpeded circulation of the work – entitles the owner of a copy of a work to sell or otherwise dispose of the possession of his or her copy of the work without the authority of the copyright owner.

Patent Law – Patent, in law, is a document issued by a government conferring some special right or privilege. In the United States, the term is restricted principally to patents for inventions granted under federal statute. The specific attributes of novelty of the item for which a patent is sought are called claims. A patent gives the inventor the exclusive privilege of using a certain process or of making, using, and selling a specific product or device for a specific period of time.

The patent is issued in the name of the United States under the seal of the PTO. It consists of a short title, together with a printed copy of the specifications and claims, a patent number, and a grant to the patentee, his or her heirs, and assignees for a period of 17 years. For design patents, the period of the patent is 14 years. Every patent must be applied for by the actual inventor, and, if two or more parties make an invention jointly, they must apply jointly. Patents may be transferred from one party to another, and the written assignment is recorded in the PTO.

Once a patent is granted, issues of infringement, the scope of the patent, or any other questions that arise out of the grant are within the jurisdiction of the U.S. district courts. Infringement consists of wrongfully making, using, or selling a patented invention. The law requires that patented articles be marked with the patent number; failure to do so will prevent the recovery of damages for infringement, unless the patent owner can prove that due notice of such infringement was given to the person charged with infringing the patent, who continued after such notice to make or sell the patented product. The remedy for an infringement is an action for damages or for a restraining injunction, or both. The manufacturer of an item for which a patent is sought may mark the product "patent pending" or "patent applied for"; such notice to the public affords an opportunity to others who may claim to have invented the same products to institute proceedings in the PTO to determine the originality of the claim of the applicant.

In general, a patent affords protection against infringement only within the jurisdiction of the government by which it is issued, and it is therefore necessary to secure a patent in every country in which protection is desired. Patent statutes have been enacted in most nations; the most important international treaty is the International Convention for the Protection of Industrial Property.

UNIT 4

THE INDIAN EVIDENCE ACT OF 1872 Vs INFORMATION TECHNOLOGY ACT 2000 – STATUS OF ELECTRONIC RECORDS AS EVIDENCE, PROOF AND MANAGEMENT OF ELECTRONIC RECORDS, RELEVANCY ADMISSIBILITY AND PROBATIVE VALUE OF E-EVIDENCE

Q.1. What do you mean by the term Indian Evidence Act 1872 Vs. Information Technology Act 2000 ?

Ans. The amendments in Indian Evidence Act 1872 have been made in the second schedule of the Indian ITA 2000. These amendments were made to improve the IT Act 2000. It seems that the maximum amendments have been made to the Indian Evidence Act.

The second schedule in the Indian Evidence Act was named "Amendments to the Indian Evidence Act of 1872". The amendments that were made in different sections of Indian Evidence Act 1872 to improve IT Act 2000 are as follows –

(i) In Section 3 –

(a) The words "all documents produced for the inspection of the Court" in the definition of "Evidence" would be replaced by the words "all documents including electronic records produced for the inspection of the Court".

(b) The expressions namely, *"Certifying authority"*, *"digital signature"*, *"secure electronic record"*, *"digital signature certificate"*, *"electronic form"*, *"information"*, *"electronic records"*, *"secure digital signature"*, *"secure electronic record"*, and *"subscriber"* would be inserted after the definition of *"India"* and the meaning of them will be same as assigned to them in ITA 2000.

(ii) In Section 17 – The words "oral or documentary" would be replaced by the words "oral or documentary or contained in electronic form

(iii) After Section 22 – The following sections named – "when oral admission as to contents of electronic records is relevant".

"22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question" would be inserted.

(iv) In Section 34 – The words "Entries in the books of account, including those maintained in an electronic form", for the words "Entries in the books of account", would be replaced.

(v) In Section 35 – The words "record or an electronic record" would be replaced for the word "record", in both the places, where it occurs.

(vi) For Section 39 – The following section would be replaced, named, "What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers. By "39. When any statement of which evidence is given forms part of a longer statement, or of a conversation or pan of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers evidence shall be given of so much and no more of the statements, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made".

(vii) After Section 47 – The following section named *opinion as to digital signature where relevant.*

"47A. When the court has to form, an opinion as to the digital signature of any person, the opinion of the certifying authority which has issued the Digital Signature Certificate is a relevant fact", would be inserted.

(viii) In Section 59 – The words "contents of documents or electronic record" would be replaced for the words "contents of documents".

(ix) After Section 65 – The following section named *special provisions as to evidence relating to electronic record.*

"65 A. The contents of electronic records may be proved in accordance with the provisions of Section 65 B" would be inserted.

Q.2. What is the status of electronic records as evidence, before and after IT Act 2000 ?

Ans. Electronic/computer evidence is a new term not covered in Indian Evidence Act, 1872. Hence there is a need of certain amendments in it. There

are many of the amendments in the Indian Evidence Act, 1872 by the IT Act, 2000 are not only redundant but also confusing due to this misconception in the lagislative mind.

The oral evidence (statement of a witness) and documentary evidence comes under Indian Evidence Act, 1872. Since there are two types of evidences which are recognized by the definition of evidence i.e., oral and documentary evidence. There are other things also which are considered as evidence, e.g., a gun used to commit a murder is also an evidence.

The status of evidence is given to these things and objects by the definition of 'proved' and 'fact' though they are not stated in the definition of evidence. The definition of evidence before the amendment by the IT Act, 2000 was as follows –

(i) All statement which are permitted by court or required to be made before it by witnesses, in relation to matters of fact under inquiry, such statements are known as oral evidence.

(ii) The documents which are produced for inspection of the court, are known as documentary evidence.

The definitions given above are amended after the IT Act 2000, as –

(i) All statements which are permitted by court or required to be made before it by witnesses, in relation to matters of fact under inquiry, such statements are known as oral evidence.

(ii) The documents including electronic records, which are produced for inspection of the court are known as documentary evidence.

In definitions given above the words 'including electronic records' is confusing because prior to the IT act, 2000, the electronic records were not documentary evidence.

Q.3. Write down the characteristics of electronic record.

Ans. Two of the odd characteristics of electronic records are as follows –

(i) The copy of the electronic record is practically indistinguishable from the original one.

(ii) Since the original electronic record was first generated and lies in the computer memory, therefore that computer would have to be brought to the court to prove the original electronic record by primary evidence, therefore it may be practically impossible or causing immense hardships in many cases.

Q.4. How can we prove that the given electronic record is original ?

Ans. An electronic record must be proved by producing the electronic record itself for the inspection of the court i.e., by primary evidence. In some

exceptional cases it is possible that the secondary evidence may be given relating to the documents. e.g., when the original document has been lost or destroyed or may be in possession of the person against whom the document is to be proved.

On the basis of primary and secondary evidence the original electronic are primary evidence while the computer output/prints are secondary evidence.

However it is difficult to distinguish an original electronic record from its copy, but there is a distinction in two based on legal and conceptual terms. The documents which are generated or processed in the computer system, would be the original electronic record. Therefore on the basis of principle of primary evidence, the computer system may have to be carried to the court physically for proving that electronic record is original. The court does not force a person to bring the computer/computer system in the court for proving the electronic record on which that person is relying as evidence, because our legal system is flexible. However the functionality of computer, reliability of the record and computer outputs are important aspects.

Therefore a special rule of evidence for electronic records was provided by section 65 B of Indian Evidence Act, 1872, introduced by the IT Act, 2000. In section 65 B, if certain conditions are satisfied then certain computer outputs of the original electronic record, can be admissible as documentary evidence in any proceedings without proof or production of the original electronic record.

It is stated in section 65 B that information contained in electronic record may be in any of the following computer outputs which are produced by the computer.

(i) Information which is printed on paper

(ii) Information which is stored or copied in any memory devices, such as DVD, memory card etc.

These computer outputs will also be treated as documents of evidence on satisfying certain conditions. The computer outputs given above may be produced as proof of the contents of the original electronic record without proving or producing the original electronic record.

Q.5. How can the electronic records be managed as evidence ?

Ans. If the business transactions or e-communications are managed/ maintained by the individuals, firms or corporates, as electronic records which may be required as evidence in any proceedings then it must be ensured that the conditions which are specified in section 65B are satisfied. It is also advised them to maintain existing records of compliance of the stipulated conditions

given in section 65B. The maintenance of records of compliance of the conditions stiputed is not a legal requirement. It is a legal advice only. These records would be relevant under the law of evidence and can enhance the creditibility of the compliance of section 65B of the Indian Evidence Act 1872.

Even being secondary evidence, the computer outputs, which are satisfying the required conditions in section 65B, would be considered to be a document. These computer outputs can be admissible in any proceedings as evidence of any contents of the original electronic record or of facts. In the fourth wing of the provision, the mode of proving compliance of section 65B of the Indian Evidence Act, 1872 is stated –

"A certificate can do any of the following things in any proceeding where a statement in evidence is desired to give, mean to say.

(i) The electronic record which contains the statement is identified and the manner is described in which it was produced,

(ii) If any device is involved in the production of that electronic record then it may be appropriate for the purpose of showing that the electronic record was produced by a computer by giving specification of that device,

(iii) It deals with any of the matters to which the conditions mentioned in the sub-section (2) relate,

and it should be signed by a responsible official position in relation to the operation of the relevant device or the management of the relevant activities shall be evidence of any matter stated in the certificate".

The person signing the certificate would require to prove the certificate in the court. The signing official may also be cross examined by the otherside.

Q.6. What do you understand by relevancy of E-evidence ?

Ans. It is our misunderstanding that if a computer output is admissible under section 65B then the some can be produced and proved in evidence. A computer output may be admissible or evident, even though it is secondary evidence, for representing electronic record in the court. It is sought to be proved that a fact is relevant or fact in issue, before can be allowed to be produced and proved in only proceedings. The basic principle is that evidence given in any proceeding, of existing or non-existing fact in issue and of other facts which are declared to be relevant by the Indian Evidence Act.

e.g., if a company JJ Ltd. contain the accounts as electronic record, in which the following entry is given which shows AJ Ltd. to be indebted to JJ Ltd. –

"Debtor's Account

AJ Ltd. ..... ₹200000/- (for sale and delivery of 10 HP printers on 09/08/2018 @ ₹10000/- per printer)"

In a money recovery suit against AJ Ltd., the JJ Ltd. relies upon the above given computer record, to prove that AJ Ltd. is indebted to it for ₹200000/-. The relevancy of this record must be satisfied by JJ Ltd. before the compliance of section 65B.

Section 34 in Indian Evidence Act gives the definition of relevancy as –

"Entries in books of accounts are relevant whenever they refer to a matter into which the court has to inquire, which are regularly kept in the course of business, though these statements may not be sufficient evidence alone to charge any person with liability".

So, we can say that the above entry can be relevant to evidence, but not sufficient, to prove the debt without other evidence.

When a fact is so connected to another as provided in the Indian Evidence Act, 1872, then the fact is said relevant. When a fact in issue is connected with the facts to form the part of the same transaction then the facts are known as relevant facts.

Q.7. Write a short note on admissibility of electronic record.

Ans. The admissibility of a fact is also to be shown as well as relevancy before any evidence of the same can be cited in any proceedings. Simply admissibility is the permission to cite the evidence. There is a big misunderstanding that admissibility and relevancy are synonyms while their legal implications are different. There are many facts that may be admissible but may not be relevant, e.g. In cross-examination, to charge the credit of a witness with crime, the questions permitted to put, though not relevant to the controversy, are yet admissible. Or an e-mail sent by a client to his advocate saying that the forgery has been committed by him and now he wish that advocate defend him. Though this communication is relevant and protected from disclosure but not admissible. Another example, when a person makes a confession to a police officer then it is relevant but is not admissible in evidence. However when the proofs are discovered in consequences of information received from the accused person of offence, in the custody of a police officer and whether it amounts to a confession or not, so much of such information is distinct from facts discovered, may be proved. For citing the evidence, the addmissibility of a fact can be shown, without any exception. Even there are exceptions where if a fact is not relevant to the controversy, is considered as admissible. Hence it can be led in evidence.

Q.8. What do you mean by authorship of an electronic record ?

Ans. The facts which are obtained to be proved by the electronic record for the test of admissibility and relevancy and compliance for admissibility of a computer output under section 65B are satisfied, then after satisfying these facts in the next step we have to prove the authorship of the electronic record. The author of an electronic record is also a person who may give the certificate that the person is occupying a responsible official position in respect to operation of the computer. When the computer was regularly used to store or process information, the management of the activities regularly carried on during the period, then the evidence of authorship would be given by such person.

If the author of the electronic record is a person other then the above said person then the other person would have to give the evidence of the authorship of electronic record. For proving a document, the general method is to call the person who had executed the document, as a witness. The person would be require to proved execution, who executed the electronic record, or who is otherwise familiar with the execution. The digital signatures would be required to be proved as evidence, if an electronic record has been signed digitally.

The contents are proved as the authorship of a document. Though it should be kept in mind that there is a distinction between the facts and the events in the contents. The definition of fact under section 3 of the Indian Evidence Act, is –

(i) If by sensing any thing, state of thing or relation of thing is being perceived.

(ii) If a person is concious of any mental condition.

Q.9. What is the probative value of electronic evidence ? Also give the types of e-evidence.

Ans. The weight to be given to evidence, which is to be judged with regard to circumstances and facts of the case. Depending upon the facts of each case, the value to be assigned to any evidence is for the court to decide. If a fact is believed to either exist by court or its existence is considered so probable that a sensible man ought, to act upon supposition that it exists, under the circumstances of a particular case. e.g., if a person claims the ownership of Red Fort, by a statement in an e-mail message sent to other person by him/her, then the probative value for this statement, would be nothing.

There is also an importance of computer generated evidence in determining its probative value. The computer generated evidences are classified as real, rumour (hearsay) and derived.

The calculations which are done by the computer using programs and softwares itself is known as real evidence. e.g., a computer software calculates the EMI for loan account from the principle, rate of interest and time period. This computation is described as most satisfactory kind of evidence and it's computation is real evidence. The informations supplied to a computer by external sources is known as rumour (hearsay) evidence, e.g., number of EMI paid, amount paid etc. are external informations which are supplied to the computer by operation.

The result generated from real and hearsay evidence is derived evidence, e.g., loan amount due to pay, number of EMIs to be paid etc. are derived because calculation is used with information supplied by external sources.

Evidence which is not direct is hearsay evidence. The rule against hearsay evidence is not restricted to oral statement and also applies to documents. As a rule hearsay evidence is not admissible in any proceedings.

PROVING DIGITAL SIGNATURES, PROOF OF ELECTRONIC AGREEMENTS, PROVING ELECTRONIC MESSAGES

Q.10. What is a digital signature ? What are its components and its applications ? ***(R.G.P.V., Dec. 2010, June 2011)***

Or

Explain digital signature. ***(R.G.P.V., Dec. 2004, 2005)***

Or

Write short note on – Digital signatures.

(R.G.P.V., June 2006, Dec. 2015)

Ans. A digital signature is a document or file attachment that gives proof that the document or file has not been modified since creation. Digital signatures are same as handwritten signatures. For instance, you draw up your will, and when it is completed and fulfills certain legal criteria you attach your written signature. Your signature is witnessed by others to certify it really was you who signed. Later, your attached signature is used to verify the authenticity of the content.

A digital signature is created by taking a hash total for a document or file and then encrypting it using a sender's private key. Then the digital signature is attached to the original material and the material is sent. This is shown in fig. 4.1.

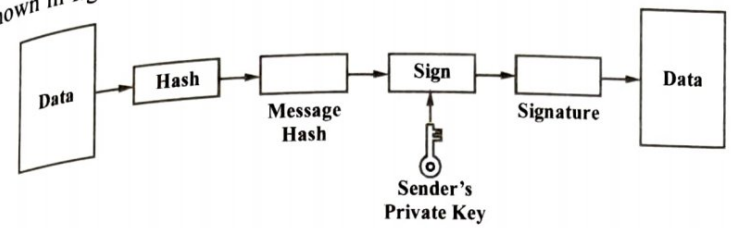


Fig. 4.1 Creating a Digital Signature

The use of public and private keys determines that who can create the signature and who can verify it. In fig. 4.1, the sender's private key was used to encrypt, so a publicly distributed key will be used to decipher. This is shown in fig. 4.2.

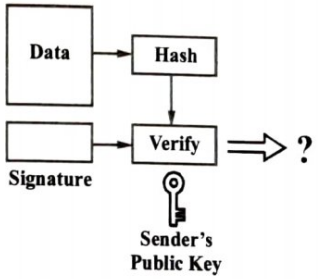


Fig. 4.2 Using a Digital Signature at the Receiver

Applications – There are several applications of cryptography in network security. Most of these applications use public keys directly or indirectly. For using a public key, a person should prove that he actually owns the public key. That is why, the idea of certificates and certificate authorities (CAs) has been developed. The CA must sign the certificates to be valid. Such a proof is provided by digital signatures.

Now-a-day's protocols using the services of CA are IPSec, SSL/TLS and S/MIME. PGP protocol uses certificates.

Q.11. Discuss the components of digital signature. (R.G.P.V., Nov. 2019)

Ans. Refer to Q.10.

Q.12. What are the requirements for a digital signature ? Also give properties of digital signature.

Ans. We can formulate the following requirements for a digital signature –

(i) The signature must be a bit pattern that depends on the message being signed.

(ii) The signature must use some information unique to the sender, to prevent both forgery and denial.

(iii) It must be relatively easy to produce the digital signature.

(iv) It must be relatively easy to recognize and verify the digital signature.

(v) It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.

(vi) It must be practical to retain a copy of the digital signature in storage.

A digital signature should have the following properties –

(i) It must verify the author and the date and time of the signature.

(ii) It must authenticate the contents at the time of the signature.

(iii) It must be verifiable by third parties, to resolve disputes.

Q.13. What are the basic functions of a signature ?

Ans. For authenticating or executing a document, putting a mark or writing of one's name is referred to as signature. The basic functions of signature are as follows –

(i) Authentication – The signatory acknowledges that he/she authorizes and adopts the text in some meaningful way by signing a document.

(ii) Identification – The signatory authority identifies himself/herself by the unique style of writing his name or mark, by signing the document.

(iii) Binding – If a person sign the document then he/she is bounded to the intent of that document.

(iv) Security – Everyone has different style of writing his/her name or putting a mark, so this individual style of signing provides security against forgery.

(v) Evidence – An evidence of above said identification, authentication and of being bound to the signed document, is a signature.

The above said functions are important for commercial transactions. Since e-commerce is growing at a rapid speed, so the parties which are involved in e-transactions needed a confident system for dealing with each other. Therefore an alternative was developed for cyber world instead of physical signature on paper, because signature plays a vital role in e-commerce. Hence the concept of digital signature was in existence. *The functions and purpose of digital signatures are same.*

Q.14. What is idea behind certification authority hierarchy ?

(R.G.P.V., June 2016)

Ans. A certification authority is a system that can validate a certificate. The authority of acting as a CA has to be with somebody who everybody trusts. Thus, a CA has the authority to issue digital certificates to individuals and organisations, which want to use those certificates in asymmetric key cryptographic applications.

Q.15. Discuss the concept of digital certificates.

Ans. A small computer file is known as a digital certificate. For example, my digital certificate will be a computer file with the file name like ankit.cer where .cer indicates the first three characters of the word certificate. The file extensions can be different. Just as my passport specifies the association between me and my other characteristics like full name, nationality, date and place of birth photograph and signature, my digital certificate specifies the association between me and my public key. Fig. 4.3 shows the concept of digital certificates. It is noted that this is only a conceptual view and does not show the actual contents of a digital certificate.

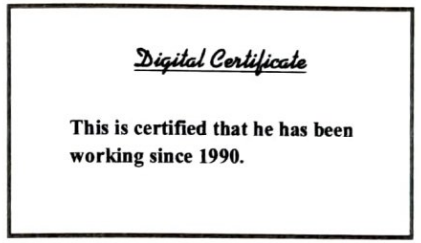


Fig. 4.3 Conceptual View of a Digital Certificate

It has not been specified who is officially approving the association between a user and the user's digital certificate. Clearly, it has to be some authority in which all the concerned parties have trust and belief. Suppose a case where our passports are not issued by a government office, but by an ordinary shopkeeper. Would we trust the passports ? Likewise, digital certificates must be issued by some trusted entity. Otherwise there will be no trust on anybody's digital certificate.

We know that a digital certificate establishes the relation between a user and her public key. Hence, a digital certificate must have the user name and the user's public key. This will prove that a particular public key is related to a particular user. In addition, what does a digital certificate keep ? Fig. 4.4 shows a simplified view of a sample digital certificate.

A few interesting things are noted here. Firstly, my name is shown as subject name. In fact, any user's name in a digital certificate is always referred to as subject name. Second is serial number. We shall see what it means in due course of time. The certificate also keeps other pieces of information, like the

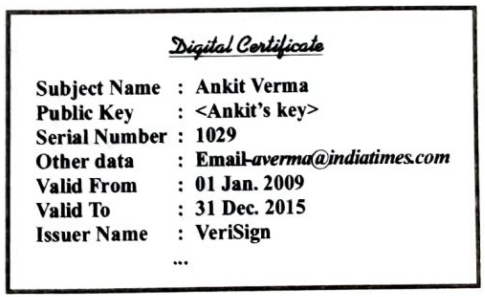


Fig. 4.4 Example of a Digital Certificate

validity date range for the certificate and who has issued it (***issuer name***). Fig. 4.5 shows the meanings of these pieces of information by comparing them with the corresponding entries in my passport.

Passport Entry	*Corresponding Digital Certificate Entry*
Full Name	Subject Name
Photograph and Signature	Public Key
Passport Number	Serial Number
Valid From	Same
Valid To	Same
Issued By	Issuer Name

Fig. 4.5 Similarities between a Passport and a Digital Certificate

Figure shows that the digital certificate is just same as passport. Every digital certificate has a unique serial number just as every passport has a unique passport number. No two passports can have the same passport number. Likewise, no two digital certificates can have the same serial number.

Q.16. What is a digital certificate ? What is the process of obtaining a digital certificate ? ***(R.G.P.V., Dec. 2010, June 2011)***

Ans. **Digital Certificate** – Refer to Q.15.

The steps involved in certificate creation are as follows –

(i) Key Generation – The action starts with the subject (that is, the user/organization) who needs to get a certificate. There are two different methods for this purpose –

(a) The subject can generate a private key and public key pair with the help of some software. Usually this software is a part of the Web browser or Web server. Alternatively, special software programs are used for this. The subject must contain the private key thus generated a secret. Then the subject sends the public key as well as other information and evidences about herself to the RA. Fig. 4.6 shows this.

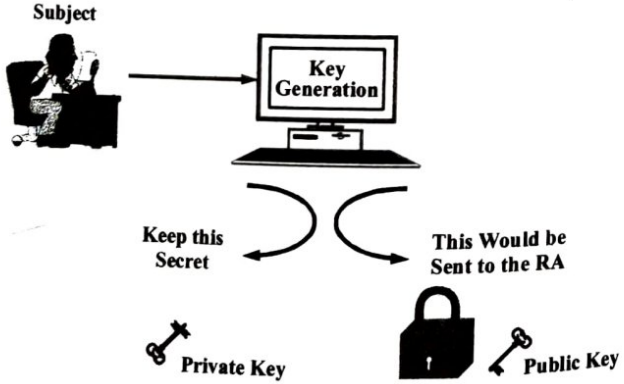


Fig. 4.6 Subject Generating its Own Key Pair

(b) Alternatively, the RA can create a key pair on the subject's behalf. This can occur in cases where either if a particular requirement demands that all the keys must be centrally generted and distributed by the RA for the ease of enforcing security policies and key management or the user is not aware of the technicalities involved in the generation of a key pair. Of course, the major drawbacks of this approach are the possibility of the RA knowing the private key of the user, as well as the scope for this key to be exposed to others while in transit after it is generated and sent to the suitable user. Fig. 4.7 shows this.

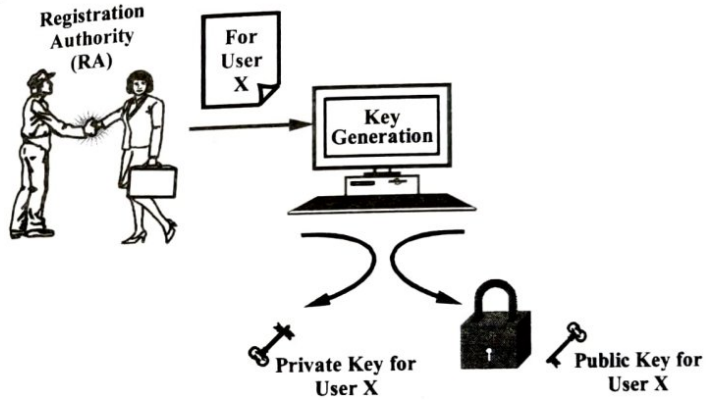


Fig. 4.7 RA Generating a Key Pair on Behalf of the Subject

(ii) Registration – This step is needed only if the user creates the key pair in the first step. If the RA creates the key pair on the user's behalf, this step will also be a part of the first step itself.

It is assumed that the user has created the key pair, the user now sends the public key and the associated registration information and all the evidence related herself to the RA. For this purpose, the software provides a wizard in which data is entered the user and when all data is correct, submits it. Then this data goes over the network/Internet to the RA. The certificate requests format has been standardized and is known as Certificate Signing Request (CSR). This is a Public Key Cryptography Standards (PKCS). The CSR is also known as PKCS#10.

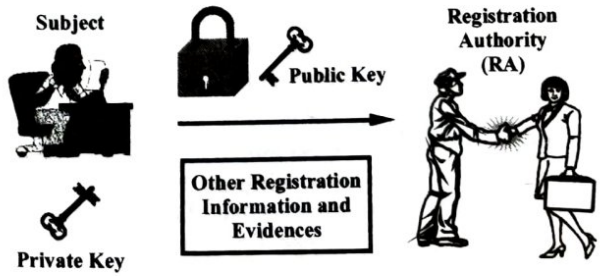


Fig. 4.8 Subject Sends Public Key and Evidences to the RA

However, the evidence, may not be in the form of computer data and usually comprises of paper-based documents like a copy of the passport or business documents or income/tax statements, etc. Fig. 4.8 shows this.

(iii) Verification – After the registration process, the RA verifies the user's credentials. This verification is done in two respects, as follows –

(a) Firstly, the RA wants to verify the user's credentials like the evidences provided are correct and acceptable. If user is an individual user, then simpler checks, like verifying the postal address, email id, phone number, passport or driving license details can be enough. If it is actually an organization, then the RA would perhaps like to check the business records, historical documents and credibility proofs.

(b) Secondly ensure that the user who is requesting for the certificate does indeed keep the private key corresponding to the public key that is sent as a part of the certificate request to the RA. This is most important, since, there must be a record that the user keeps the private key corresponding to the given public key. Otherwise, this can cause legal problems This check is known as checking the Proof Of Possession (POP) of the private key. The RA uses the following approaches to perform this check –

(1) The RA can want that the user must digitally sign her Certificate Signing Request (CSR) using her private key. If the RA can verify the signature properly with the help of the public key of the user, the RA can believe that user indeed keeps the private key.

(2) Alternatively, at this stage, the RA can generate a random number challenge, encrypt it with the user's public key and send the encrypted challenge to the user. If the user can properly decrypt the challenge using her private key, the RA can believe that the user keeps the right private key.

(3) The RA can actually create a dummy certificate for the user, encrypt it using the user's public key and send it to the user. The user can decrypt it only if she can decrypt the encrypted certificate and get the plaintext certificate.

(iv) Certificate Creation – Assuming that all the steps so far have been successful, the RA provides all the details of the user to the CA. The CA verifies itself (if needed) and generates a digital certificate for the user. There exist programs for creating certificates in the X.509 standard format. The CA transmits the certificate to the user and also keeps a copy of the certificate for its own record. The CA's certificate copy is kept in a certificate directory. The CA maintains this central storage location. The contents of the certificate directory contents are same as that of a telephone directory. This facilitates for a single-point access for certificate management and distribution.

No single standard exists that interprets the structure of a certificate directory. However, the X.500 standard is growing as a popular alternative. It

permits the storage of not only the digital certificates, as well as the information about servers, printers, network resources, the user's personal information, like telephone numbers/extensions, email id's, etc. at a central place in a controlled way. From this central repository, the directory clients can request for and access information with the help of a directory access protocol, like the Lightweight Directory Access Protocol (LDAP). LDAP permits users and applications to access X.500 directories, based on their privileges.

Then the CA sends the certificate to the user. This is attached to an e-mail or the CA sends an email to the user, informing that the certificate is ready and that the user should download it from the CA's site.

Q.17. How can we verify the digital signatures ?

Ans. The Indian IT Act 2000 amended from the Indian Evidence Act 1872, describes that if the digital signature of any person is illegal to be affixed to an electronic record, then such digital signature is to be proved by the person, except the secure digital signature. Section 73A introduce in the Indian Evidence Act 1872, defines to court how digital signatures are verified.

To verify digital signature produced by the subscriber the court may ask to the subscriber –

(i) That the controller or the certifying authority have to produce digital signature certificate.

(ii) To verify the digital signature the court may ask any other person for applying the public key.

The opinion of the certifying authority which issued the digital signature certificate will be the relevant fact when court form an opinion about digital signature of a person.

In order to ascertain, that a digital signature of person who claims it to be affixed, the court has been empowered, to direct –

(i) The controller or the certifying authority to produce the digital signature certificate.

(ii) To verify the digital signature claimed to be affixed by that person by asking any other person to apply the public key listed in digital signature certificate.

To prove the digital signatures, the digital signature certificate plays an important role as seen in both above said conditions. The IT Act 2000, introduced the section 85C of Indian Evidence Act, describes that unless the contrary is proved, that the information contained in digital signature certificate is correct while the digital signature certificate is accepted by the subscriber. The information provided by the subscriber, which has not been verified, is not included in it. Hence the person who is relying on the information will have to prove this information in any proceedings where proof of it is essential.

The secure digital signatures have a special legal status. It can be verified that a digital signature, at time wen it was affixed, was –

(i) Unique to the subscriber who was affixing it

(ii) Capable of identifying such subscriber

(iii) Created in a manner or using a means under the exclusive control of the subscriber.

Then such digital signature is assumed to be a secured digital signature.

Until the contrary is proved, the court shall assume that it has been affixed with the intention of signing or approving the electronic record, where a secure digital signature is involved.

Q.18. What do you mean by proof of electronic agreements ?

Ans. The electronic agreements can be classified into the following categories –

(i) Both parties affixed digital signature on which is electronic agreement.

(ii) Electronic agreement between the parties sending messages through e-mail.

(a) The party sending message with digital signature.

(b) The party sending message without digital signatures.

The section 85A of Indian Evidence Act 1872 has been assumed to included the definition for electronic agreements, signed by both parties –

"Every electronic record seems to be an agreement containing the digital signatures of the parties which is concluded by affixing the digital signature by both parties. This will be assumed by court".

Here the word 'unless the contrary is proved' is not included but the concept is not conclusive and rebuttable yet. It implies that this is the responsibility of a person to, prove that the agreement was not concluded by affixing the digital signatures.

Over the status of electronic records, the proof of terms and conditions was an important issue, after and before the IT Act 2000. The terms of a contract, according to the section 91 of the Indian Evidence Act 1872, are reduced to form a document. In the proof of terms of such contracts no evidence can be given. However, oral evidence which are admissible can be used to prove the statement of other facts in a contract.

There is an confusing issue that whether section 91 would be applied to an electronic agreement because of the status of electronic records as documentary evidence prior to and after the IT Act. It may be a fact that the legislature does not want to apply this phenomena to electronic agreement because the section 91 of the Indian Evidence Act 1872, has not been amended as the sections 17, 34, 35 etc. While on the other hand even before IT Act, 2000, the electronic records were documents, so the section 91 would be applied to electronic agreement also. Hence, for proving the terms and conditions of an e-agreement, no evidence can be given except the e-agreement itself. The digital signatures upon the e-agreements would be required to prove because of principle of proving digital signature.

Q.19. What are the rules of digital evidence ?

Ans. There are a number of sources like sized computer hard drives and backup media, real-time e-mail messages, chat room logs, Internet service provider records etc. from where the digital evidences originate. The rules for collecting the digital evidences are as follows –

(i) We can collect the digital evidence by engaging the appropriate incident handling and law enforcement personnel.

(ii) By capturing a picture of the system as accurate as possible.

(iii) We can collect digital evidences by keeping detailed notes with date and time, and an automatic transcript should be generated if possible. Our notes and printouts should be signed and dated.

(iv) We should note the difference between the system clock and coordinated universal time (UTC). For each timestamp it should be indicated whether the UTC or local time is used.

(v) We should check by outlining all actions we took and at what times. For this detailed notes will be needed.

(vi) The data collected should be changed at minimum rate. This is not limited to the content changes; we should avoid updating file or directory access times.

(vii) When we are confused to choose between collection and analysis, then we should do collection first and analysis later.

(viii) Our procedures should be implementable and should be tested to ensure feasibility, particularly in a crisis, with aspect to an incident response policy.

(ix) A systematic approach should be adopted to follow the guidelines laid down in our collection procedure, for each device. Since the speed is a critical issue so when we need to examine a number of devices, then we should spread our work among our team to collect the evidence in parallel.

(x) Evidences should be collected in volatile to less volatile manner, the order of volatility is as follows –

(a) Registers and cache memory because as room the power is switched off the data will be lost.

(b) Routing table, ARP cache, process table, kernel statistics and memory are also volatile.

(c) Temporary file systems are less volatile than above.

(d) Disk is less volatile than above given.

(e) Remote logging and monitoring data that is relevant to the system.

(f) Physical configuration and network topology.

(g) Archival media is least volatile means data will be stored even after the power is switched off.

Q.20. What do you mean by proving electronic messages ?

Ans. Electronic messages are admissible as documentary evidence and these are also electronic records. Here we shall study some aspects of e-messages under the law of evidence. Since use of Internet is increasing day by day, so the e-mail evidence can also be presented to the court in civil and criminal trials. Although the electronic message technology is an efficient, easy to use and cost-free mode of communication, but the probative value of an electronic message is a question. Today anyone can open e-mail very easily in the names of other persons and send the message to each other by sending messages and can create violence among them. Thus the e-mail system is vulnerable to misuse and abuse.

The concept of digital signature enhances the evidentiary credibility of e-messages on which digital signatures are affixed. The asymmetric crypto system is used to encrypt the data and is recognized as the digital signatures under the IT Act, 2000, is unique to the data and subscriber. Since the signatory is identified by the digital signatures, so the digital signatures can lift the evidentiary value of the signed e-message. The acknowledgement of receipt of an electronic record and identification of the originator and addressee is defined in the section 12 of the IT Act 2000. Hence, proof of these ingredients may be applicable to the factual matrix. These ingredients would be good evidence for identifying the originator and addressee and sending or receiving of the e-message, which seeks to be proved.

The section 12 of IT Act 2000 is described as given below –

(i) If the originator of the acknowledgement has not agreed with the addressee that the receipt of electronic record be given in a particular form or by a particular method, then an acknowledgement may be given by –

(a) Any communication by the addressee, automated or otherwise.

(b) Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(ii) Where if the originator has specified that the electronic record shall be binding only on receipt of an acknowledgement of such electronic record by him, then the electronic record shall be considered to never sent by originator unless the acknowledgement has been received.

(iii) Where if it has not specified that the electronic record shall be binding only on receipt of acknowledgement and the acknowledgement has not been received by the originator within the specified time or agreed or if no time has been specified or agreed or if agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgement has been received by him and specifying a reasonable time by which the acknowledgement must be received by him. If with in the above said time limit no acknowledgement is received, he may treat the electronic record as though it has never been sent, after giving notice to addressee.

Q.21. What is the role of digital signature in digital evidence ?
(R.G.P.V., Nov. 2018)

Ans. To define electronic signature a new section named section 3A was introduced in Indian IT Act, by retaining section 3 of digital signatures. An electronic signature is an alternative propose of digital signature. Both of these can be used for authentication of digital evidence (electronic record). So the certifying authorities are needed to accommodate for both digital signature and electronic signature.

Neverthless anything contained in section 3 but according to provision of subsection (2), any electronic record (digital evidence), may be authenticated by a subscriber, using electronic signature, that are considered reliable and may be specified in the second schedule.

The electronic signature or digital signature technique shall be considered reliable if –

(i) At the time of signing the authentication data or signature creation were under the control of signatory, or as the case may be, the authenticator or of no other person.

(ii) After affixing digital signature, any alternation made to the digital signature, are detectable.

(iii) After authenticating the information by digital signature any alteration made to it are detectable.

(iv) The signature creation data or the authentication data linked to the signatory are within the context in which they are used.

For the purpose of ascertaining whether the person by whom the digital signature is claimed to have been affixed or authenticated, the Central Government may prescribe the procedure. It should be notified in Official Gazette of the Central Government to add or omit digital signature and the procedure for affixing such signature from the second schedule.

Q.22. How can we check the validity of digital evidence ?
(R.G.P.V., Nov. 2018, 2019)

Ans. The process used in the case of digital evidence copies the process used for paper evidence, this is only logical. The process must be documented reliable and repeatable since each step requires the use of tools or knowledge.

To understand the digital evidence is both legal and technical problem. Actually both of these facts are related. The law specifies under what conditions what can be seized, from where and from whom. It needs to determine what particular piece of digital evidence is needed for checking validity, i.e. is it a particular file or an executable program or a word processing document etc. It may also required to check whether a particular piece of evidence is physically located. It may also be necessary to show a technical basis for obtaining the legal authority to search. There are a number of context involved in actually validating a piece of digital evidence, three of them are as follows –

(i) Physical Context – It must be definable in its physical form, i.e., it should reside on a specific piece of media.

(ii) Logical Context– It must be identifiable as to its logical position, i.e., where does it reside relative to the file system.

(iii) Legal Context – We must place the evidence in the correct context to read its meaning. This may require for looking at the evidence as machine language.

The path taken by digital evidence is shown in fig. 4.9 given below –

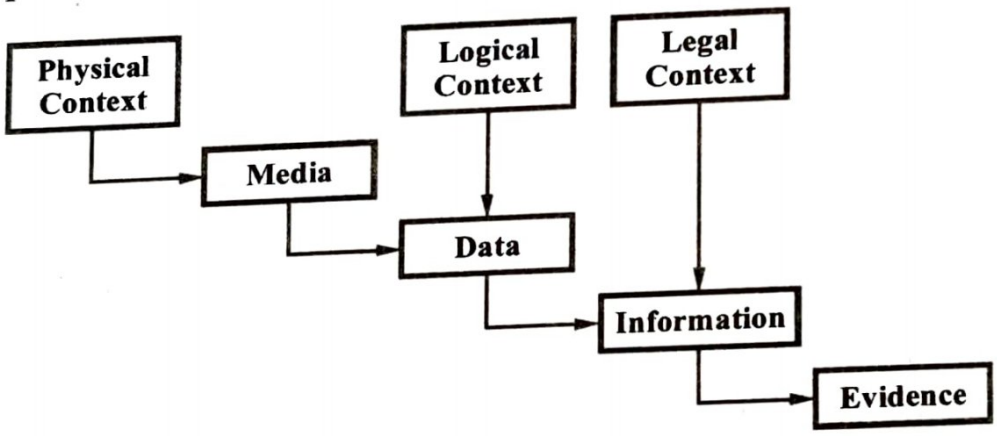


Fig. 4.9 Path of Digital Evidence

Once the extraction of digital evidence from a number of sources such that hard drives of seized computer, real-time e-mail messages, Internet service provider records, webpages, digital network traffic etc., is completed, the validity of extracted data is checked.

A digital evidence is valid if it is admissible in the court or before law enforcement agencies for jurisdiction and accepted. If the court or law enforcement agencies accept the digital evidence as evidence for any crime then the digital evidence is valid.

UNIT 5

TOOLS AND METHODS IN CYBERCRIME – PROXY SERVERS AND ANONYMIZERS, PASSWORD CRACKING, KEY LOGGERS AND SPYWARE, VIRUS AND WORMS, TROJAN HORSES, BACKDOORS

Q.1. What is proxy server ? How attackers attack on proxy server ?

Ans. A computer, which acts as an intermediary for connections on a network with other computers on same network, is known as proxy server.

The attackers try to establish a connection with the target system by connecting to a proxy server, through existing connection with proxy. Doing so the attacker is enable to surf on the web parallely and/or hide the attack. A client requests some services, while connects to the proxy server, available from a different server. The resources are provided to the client, when proxy server evaluates the request, by establishing connection to the respective server and/or requests the required service on behalf of client. A proxy server can allow an attacker to hide his ID.

The purposes of proxy server are as follows –

(i) Proxy server keep the systems hidden it means it secure the systems.

(ii) It uses caching to speed up access to a resource. It caches web-pages from web servers.

(iii) Unwanted contents are filtered by some special proxy servers.

(iv) To enable to connect number of computers on the Internet, whenever one has only one IP address, proxy server can be used as IP address multiplexer.

A proxy server has an advantage that its cache memory can serve all users. If different users are requesting one or more websites then it is likely to be in proxy server's cache memory, which will improve user response time.

Q.2. What is anonymizer ? How anonymizers work ? (R.G.P.V., Nov. 2018)

Ans. A tool that attempts to make activity on the Internet untraceable is known as anonymous proxy or anonymizer. It protects user's personal information by hiding the source computer's identifying information and accesses the Internet on user's behalf. The services that make web surfing anonymous by utilizing a website that acts as a proxy server for the web client are also known as anonymizers. The Lance Cottrell developed first anonymizer software tool in 1997. When user surf on Internet the anonymizer hides/ removes all the information from user's computer.

Q.3. What do you mean by password cracking ? Explain in brief.

Ans. Like a lock, password is a key to get an entry into computerized systems. The process of recovering password from the data that have been stored in or transmitted by a computer, is known as password cracking. Generally a common approach is followed by an attacker for making guesses for the password. The purposes of password cracking are as follows –

(i) It can be used to recover a forgotten password.

(ii) System administrators can use password cracking in preventive manner, to check for easily crackable passwords.

(iii) Password cracking can be used to access a system for which attacker is not authenticated.

An attempt to logon with different passwords is known as manual password cracking. In manual password cracking following steps are followed–

(i) A valid user account is found out

(ii) List of possible passwords is created

(iii) Passwords are ranked from high to low probability

(iv) Try again and again to get a successful password.

Sometimes password can be guessed with knowledge of the user's personal information. Some guessable passwords are as follows –

(i) The words such as password, admin and administrator etc.

(ii) Series of letters from the QWERTY keyboard e.g., qwerty, qwertyuiop, asdf, etc.

(iii) User's name or login name can be used to guess the password.

(iv) User's pet name can also be used to guess password.

(v) User's D.O.B., birth place etc. can be used to guess the password.

(vi) Attackers can use user's mobile number, vehicle number, residence phone number etc. to guess the password.

(vii) Sequence of number such as 123456, 1234 can also be used to guess the password.

An automated program can also be executed to try each password in a list. It is called manual cracking and considered as time consuming and usually not effective.

Q.4. Classify the password cracking attacks and explain each.

Ans. Password cracking attacks are classified into the following categories –

(i) Online Attacks – An automated program which is also known as script file can be created and will be execute by attacker to try each password in a list. Man-in-the middle attack is very popular attack. It is also called as "bucket-brigade attack" or sometimes "Janus attack". In this attack, a connection is established between a victim and the server to which a victim is connected, by eavesdropping the network, and when the victim client try to connect to the server, then it is connected to the fraudulent server instead of actual, and hence MITM server intercepts the call, hashes the password and passes the connection to victim server. Using this attack passwords of public e-mail accounts and passwords for financial website which are gaining access to bank websites can be cracked.

(ii) Offline Attacks – In offline attacks systems are accessed physically, and the password files are copied from computer to removable media instead of target the offline attacks are applied from location, where these passwords reside. Some types of offline attacks are given below –

(a) Dictionary Attack – As the name implies in this attacker attempts to match all the possible words from dictionary to access password, such as Admin.

(b) Hybrid Attack – In hybrid attacks a sequence of letters and numbers is used to guess the password such as ABC123.

(c) Brute Force Attack – In this attack all possible permutation combination of letters, symbols and special characters are applied to guess the password.

(iii) Non-electronic Attacks – These types of attacks are not performed on computers. These attacks are based on physical movement of a victim, e.g. shoulder surfing in which attacker keep watch over a person's shoulder while he/she logs into the system.

Q.5. What is keylogging ? Explain types of keyloggers.

Or

Write a short note on keyloggers. ***(R.G.P.V., Nov. 2018)***

Ans. When a person who is using the keyboard is unaware that the keys struck on a keyboard are noted by others, is known as keylogging. Keystroke logging or keylogging is the easiest way to hack the passwords and monitor the victim's IT savvy behaviour. There are following types of keyloggers –

(i) Software Keyloggers – The software programs installed on the computer and located between the OS and the keyboard hardware and records

every key stroke, are known as key software keyloggers. User has no knowledge about the software keyloggers because these are installed on a system by Trojans or viruses. Such tools are generally installed on unsecure systems by the attackers. Now the attacker can get victim's information very easily. Usually two files are get installed on a computer by the attacker in the same directory – a DLL file and an EXE (Executable) file that installs the DLL file and triggers it to work. All recordings are done by DLL.

(ii) Hardware Keyloggers – These are small hardware devices which are connected to the computer or keyboard without knowledge of user. The computer system should be accessed physically to install hardware keyloggers. This device saves every keystroke in a file or in the memory of hardware device. This type of devices are installed on ATM machines to capture ATM card's PINs by saving each keypress on the keyboard.

(iii) Antikeylogger – The keyloggers installed on the computer system can be detected and removed by antikeylogger. Some of the advantages of antikeyloggers are as follows –

(a) The installation of keyloggers can be detected by antikeyloggers since the firewalls are not able to do so.

(b) Any updates of signature bases to work effectively is not required by antikeyloggers.

(c) ATM and Internet banking frauds can also be prevented by antikeyloggers.

(d) Identity theft is prevented by this.

Q.6. Write short note on spyware. ***(R.G.P.V., Nov. 2019)***

Ans. Spywares are also installed on computers and collect information about user without their knowledge. These are types of malware. Sometimes spywares are installed by the owner of a shared/public computer to secretly monitor other users.

As the name implies spyware means secret monitoring of users. All the personal informations of users are collected by spywares such as Internet surfing habits/patterns, websites visited etc. Internet surfing activities can be changed by installing another utility on the victim's computer. Computer settings, resulting in slower Internet connection speeds and slowing of response time, can also be changed by spywares.

Some of the spywares are given below –

(i) 007 Spy – The URL of websites that are visited on Internet can be recorded by this spy. It has powerful keylogger engine to capture all passwords.

(ii) eBlaster – It is a powerful spy. It records all e-mails sent and received, various files downloaded/uploaded, record program searches and any other activities besides the keylogging and website watching.

(iii) Flexispy – This tool may be installed on mobile phones. After installing this tool, it secretly records the conversation on phone and transfer it to a specific e-mail address.

(iv) Wiretap Professional – An application that is used for monitoring and capturing all activities on the system is called wiretap professional spy. Internet activities can also be captured by it. The keystrokes and passwords are also recorded by it.

(v) Spector Pro – All the chats and instant messages are captured by this spy. This spy also captures all sent/received mails. Besides this it also captures all websites visited.

Q.7. Write short note on viruses. ***(R.G.P.V., June 2005, Dec. 2006)***

Ans. A virus is a program that can "infect" other programs by modifying them. The modification includes a copy of the virus program, which can then go on to infect other programs.

Biological viruses are tiny scraps of genetic code – DNA or RNA – that can take over the machinery of a living cell and trick it into making thousands of flawless replicas of the original virus. Like its biological counterpart, a computer virus carries in its instructional code the recipe for making perfect copies of itself. Lodged in a host computer, the typical virus takes temporary control of the computer's disk operating system. Then, whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program. Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network. In a network environment, the ability to access applications and system services on other computers provides a perfect culture for the spread of a virus.

A virus can do anything that other programs do. The only difference is that it attaches itself to another program and executes secretly when the host program is run. Once a virus is executing, it can perform any function, such as erasing files and programs.

Q.8. Discuss the virus characteristics.

Ans. When a virus-infected program is run, the virus code is executed first. One of the first tasks of virus code is to seek other programs not yet infected and then pass on the infection to one or more of them. A truly malicious virus may then perform actions such as deleting certain files. An innocuous virus may attempt something benign like printing a "hello world" message. Execution of the virus code is usually followed by execution of the host's original program.

All the virus code need not be located at the start of the infected file. In some cases, virus code is both prepended and appended to the host file. Virus

code could be split into several segments and interspersed throughout the infected file using JUMP statements at the end of each virus segment. In most of these cases, the size of the infected program is larger than the original host program. This helps anti-virus software to detect infected code.

To evade detection, some viruses modify the ***file service interrupt handler*** that returns attributes of files. By so doing, the service handler may be programmed to return the uninfected length of the file. Another technique is to use ***compression*** so that the length of an infected file remains the same as the length of its original version. The virus writer includes a compression routine in the viral code. To infect another file, the virus first compresses that file and then prepends the virus code to the compressed file. The infected file must be uncompressed just prior to execution.

One of the characteristic features of many viruses is the set of system calls they make. System calls are used by application programs to request services of the operating system. They are made to read/write files, spawn new processes, establish TCP connections, etc. Some viruses make calls to copy their own code to other files, create/modify entries in the Windows registry, or search for e-mail. Such "suspicious" calls are often used to distinguish malicious from benign code.

Q.9. What is a compression virus ? What can you do to detect a compression virus ? ***(R.G.P.V., June 2017)***

Ans. Refer to Q.8.

Symptoms of Compression Virus Cruncher-1.0 – The primary symptons of compression virus cruncher 1.0 are as follows –

(i) Unpredictable computer behaviour.
(ii) Operating system shows unexpected error messages.
(iii) Blue screen error in windows.
(iv) Computer perform slowly.
(v) Program does not respond and display not responding error message.
(vi) Deletions of mysterious files and folder.
(vii) Spam messages being sent from your email Id without your knowledge.

Removing of Compression Virus Cruncher-1.0 – Compression virus cruncher 1.0 can be removed in the following ways –

(i) Install anti-malware software.
(ii) Window registry must be clean and update continuous.

Q.10. What are the characteristics of a virus ? Explain the working of a virus in detail. ***(R.G.P.V., Dec. 2010, June 2011)***

Ans. **Virus Characteristics** – Refer to Q.8.

A virus can be prepended or postpended to an executable program, or it can be embedded in some other fashion. The key to its operation is that the infected program, when invoked, will first execute the virus code and then execute the original code of the program. A very general structure of virus is portrayed in fig. 5.1. In this case, the virus code, V, is prepended to be infected programs, and it is assumed that the entry point to the program, when invoked, is the first line of the program.

```
        program V : =
{goto main;
    1234567;

        subroutine infect-executable : =
            {loop:
            file : = get-random-executable-file;
            if (first-line-of-file = 1234567)
                    then goto loop
                    else prepend V to file;}
        subroutine do-damage : =
            {whatever damage is to be done}

        subroutine trigger-pulled : =
            {return true if some condition holds}

main :  main-program: =
            {infect-executable;
            if trigger-pulled then do damage;
            goto next;}
next :

}
```

Fig. 5.1 A Simple Virus

An infected program starts with the virus code and works as follows. The first line of code is a jump to the main virus program. The second line is a special marker that is used by the virus to determine whether or not a potential victim program has already been infected with this virus. When the program is invoked, control is immediately transferred to the main virus program. The virus program first seeks out uninfected executable files and infects them. Next, the virus may perform some action, usually detrimental to the system. This action could be performed every time the program is invoked, or it could be a logic bomb that triggers only under certain conditions. Finally, the virus transfers control to the original program. If the infection phase of the program is reasonably rapid, a user is unlikely to notice any difference between the execution of an infected and uninfected program.

Once a virus has gained entry to a system by infecting a single program, it is in a position to infect some or all other executable files on that system when the infected program executes. Thus viral infection can be completely prevented

by preventing the virus from gaining entry in the first place. Unfortunately, prevention is extra ordinarily difficult because a virus, can be part of any program outside a system. Thus, unless one is content to take an absolutely bare piece of iron and write all one's own system and application, programs, one is vulnerable.

Most viral infections initiate with a disk from which programs are copied onto a machine. Many of these are disks that have games or simple but handy utilities that employees obtain for their home computers and then bring in and put on an office machine. Some, incredibly, are present on disks that come shrink – wrapped from the manufacturer of an application. Only a small fraction of infections begin across a network connection. Again, typically, an employee will download a game or apparently useful utility only to discover later that it contains a virus.

Q.11. What is computer virus ? How the virus spread ?

Ans Refer to Q.7 and Q.10. ***(R.G.P.V., Nov. 2019)***

Q.12. Explain various types of viruses. ***(R.G.P.V., June 2010)***

Or

Briefly describe the types of viruses. ***(R.G.P.V., Dec. 2012)***

Or

Classify the different categories of viruses. ***(R.G.P.V., Dec. 2016)***

Ans. The following categories as being among the most significant types of viruses have been suggested –

(i) Stealth Virus – A form of virus explicitly designed to hide itself from detection by antivirus software. For example, a virus that uses compression so that the infected program is exactly the same length as an uninfected version. Far more sophisticated techniques are possible. Another example, a virus can place intercept logic in disk I/O routines, so that when there is an attempt to read suspected portions of the disk using these routines, the virus will present back the original, uninfected program. Thus, stealth is not a term that applies to a virus as such but, rather, is a technique used by a virus to evade detection.

(ii) Polymorphic Virus – A virus that mutates with every infection, making detection by the "signature" of the virus impossible. This virus creates copies during replication that are functionally equivalent but have distinctly different bit patterns. As with a stealth virus, the purpose is to defeat programs that scan for viruses. In this case, the "signature" of the virus will vary with each copy. To achieve this variation, the virus may randomly insert superfluous instructions or interchange the order of independent instructions. A more effective approach is to use encryption. A portion of the virus, generally called a ***mutation engine***, creates a random encryption key to encrypt the remainder of the virus. The key is stored with the virus, and the mutation engine itself is altered. When an infected program is invoked, the virus uses the stored random key to decrypt the virus. When the virus replicates, a different random key is selected.

(iii) Parasitic Virus – The traditional and still most common form of virus. A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.

(iv) Memory-resident Virus – Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.

(v) Boot Sector Virus – Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.

Q.13. What is virus ? Explain different types of viruses. ***(R.G.P.V., Dec. 2013)***

Ans. Refer to Q.7 and Q.12.

Q.14. What is virus ? What is virus structure ? Explain the types of viruses. ***(R.G.P.V., June 2012)***

Ans. Refer to Q.7, Q.10 and Q.12.

Q.15. What are the two phases of execution of a virus ?

Ans. Viruses potentially have two phases to their execution – the infection phase, and the attack phase.

Infection Phase – When a virus executes it has the potential to infect another program. When it would infect other program is clearly not understood. Some viruses infect each time they are executed; other viruses infect only when triggered. This trigger could be anything; a day or time, an external event, a counter within the virus, and so forth. Virus writers want their programs to spread as far as possible before they are detected.

Many viruses go resident in the same or similar manner as Terminate and Stay Resident (TSR) programs. This means, the virus waits for an external event before infecting additional programs. A virus may silently lurk in memory waiting for a user to access a diskette, copy a file, or execute a program, before it begins infecting. This makes viruses difficult to analyze, because it is hard to determine the trigger condition.

Attack Phase – Just as the infection phase can be triggered by an event, the Attack Phase also has its own trigger. Not all viruses' attack, but all of them do use system resources, and frequently contain bugs.

These bugs can cause unintended negative side effects. In addition, viruses often delay revealing their presence by launching an attack only after they have had ample opportunity to spread. This means an attack could be delayed for days, weeks, months, or even years after the initial infection.

The Attack Phase is optional; many viruses reproduce without a trigger condition. However, anything that writes itself to a disk without permission is

stealing storage and CPU cycles. Viruses that "only infect", with no Attack Phase often damage programs or disks. This is not an international act of the virus, but simply the result of poorly written code.

Q.16. What is virus ? How it works ? Explain its phases of execution. ***(R.G.P.V., Dec. 2015)***

Ans. Refer to Q.7, Q.10 and Q.15.

Q.17. What are the different ways to infect computer systems through viruses ?

Ans. There are following ways viruses infect computer systems –

(i) Boot Sector Penetration – A boot sector is usually the first sector on every disk. In a boot disk, the sector contains a chunk of code that powers up a computer. In a non-bootable disk, the sector contains a file allocation table (FAT), which is automatically loaded first into computer memory to create a roadmap of the type and contents of the disk for the computer to access the disk. Viruses imbedded in this sector are assumed of automatic loading into the computer memory.

(ii) Macros Penetration – Because macros are small language programs that can execute only after imbedding themselves into surrogate programs, their penetration in quite effective. The rising popularity in the use of script in web programming is resulting in micro virus penetration as one of the fastest forms of virus transmission.

(iii) Parasites – These are viruses that attach themselves to a healthy executable programs and wait for any event where such a programs is executed. Nowadays, due to the spread of the Internet, this method of penetration is the most widely used and the most effective. Examples of parasite virus include Friday the 13th, Michelangelo, SoBig, and the Blaster viruses.

Q.18. Discuss digital immune system. ***(R.G.P.V., Dec. 2009, 2012)***

Ans. The digital immune system is a comprehensive way to virus protection developed by IBM. The motivation for this development has been the rising threat of Internet-based virus propagation.

In response to the threat posed by these Internet-based capabilities, IBM has developed a prototype digital immune system. The objective of this system is to provide rapid response time so that viruses can be stamped out as soon as they are introduced. When a new virus enters an organization, the immune system automatically captures it, analyzes it, adds detection and shielding for it, removes it, and passes information about that virus to systems running IBM AntiVirus so that it can be detected before it is permitted to run elsewhere.

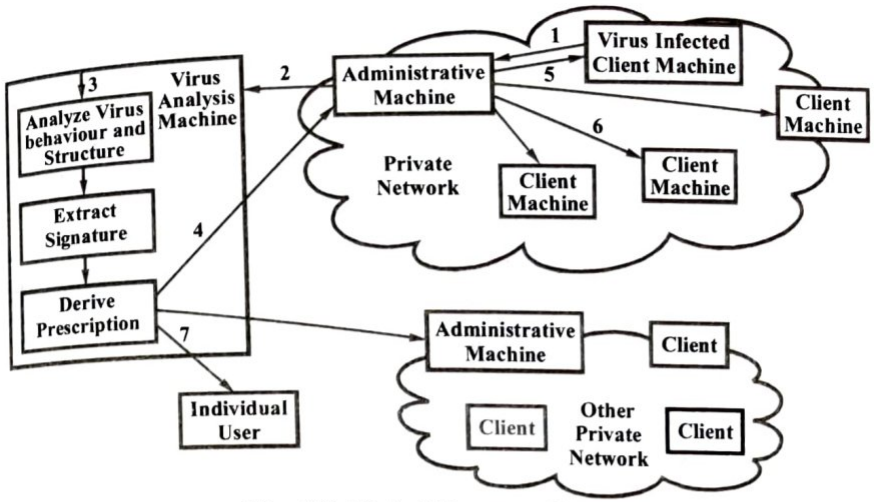


Fig. 5.2 Digital Immune System

The steps in digital immune system operation are shown in fig. 5.2 –

(i) A monitoring program on each PC uses a number of heuristics on the basis of system behaviour, suspicious changes to programs, or family signature to infer that a virus may be present. A copy of any program thought to be infected is sent by the monitoring program to an administrative machine within the organization.

(ii) The administrative machine encrypts the sample and sends it to a central virus analysis machine.

(iii) This machine creates an environment in which the infected program can be safely run for analysis.The techniques used for this purpose are emulation, or the creation of a protected environment within which the suspected program can be executed and monitored. Then, the virus analysis machine produces a prescription for identifying and removing the virus.

(iv) The resulting prescription is sent back to the administrative machine.

(v) The administrative machine sends the prescription to the infected client.

(vi) The prescription is also sent to other clients in the organization.

(vii) Subscribers around the world get regular antivirus updates that protect them from the new virus.

Q.19. What is computer virus ? How the virus spread ? How to protect against virus ? ***(R.G.P.V., Nov. 2018)***

Ans. **Computer Virus** – Refer to Q.7.

Spreading of Virus – Refer to Q.10.

Protection Against Virus – Refer to Q.18.

Q.20. Define worm. ***(R.G.P.V., Dec. 2007)***

Or

Write short note on worm. ***(R.G.P.V., Dec. 2015, Nov. 2019)***

Ans. A worm is sometimes confused with a virus. They have some similarities, the worm is code. However, it is an independent program that does not modify other programs, but reproduces itself over and over again until it slows down or shuts down a computer system or a network.

Q.21. Define the worm propagation model. ***(R.G.P.V., Dec. 2016)***

Ans. Refer to Q.20.

Worm propagation model helps us obtain insights into the factors that govern its speed. It also helps in studying the efficacy of different schemes designed to retard the spread of a worm.

Q.22. Describe three phases of worm propagation. (R.G.P.V., June 2017)

Ans. There are three phase of worm propagation – Target finding, worm transferring and infection.

Target Finding – In target finding phase, worms determine the target in different spaces.

There are four classes in which worms finds the target on the bases of space – address space.

(i) Internet Worms – Internet worms search the target in the IP space.

(ii) P2P Worms – P2P worms search the target in the P2P networks space.

(iii) E-mail Worms – E-mail worms search the target in the email address space.

(iv) Instant Messaging (IM) Worms – IM worms search the target in the IM user IDs space.

Above classification is not strict. Many worms can use two or more classes. For example, the Nimda worm is an e-mail and internet worm. Bibrog is a email and P2P worm.

Worm Transferring and Infection – Worm transfer and infection can be done manually or automatically. From high to low, human intervention degrees can be of four types – manual transfer and manual infection, manual transfer and automatic infection, automatic transfer and manual infection, and automatic transfer and automatic infection.

Fig. 5.3 shows the four worm classes of human intervention degrees. Internet worms use automatic tranferring and automatic infection via remotely exploitation in which the worms code can be transferred and executed without any human efforts. IM worms and e-mail worms uses automatic transferring and manual infection or manual transferring and automatic infection. P2P uses all four human intervention degrees.

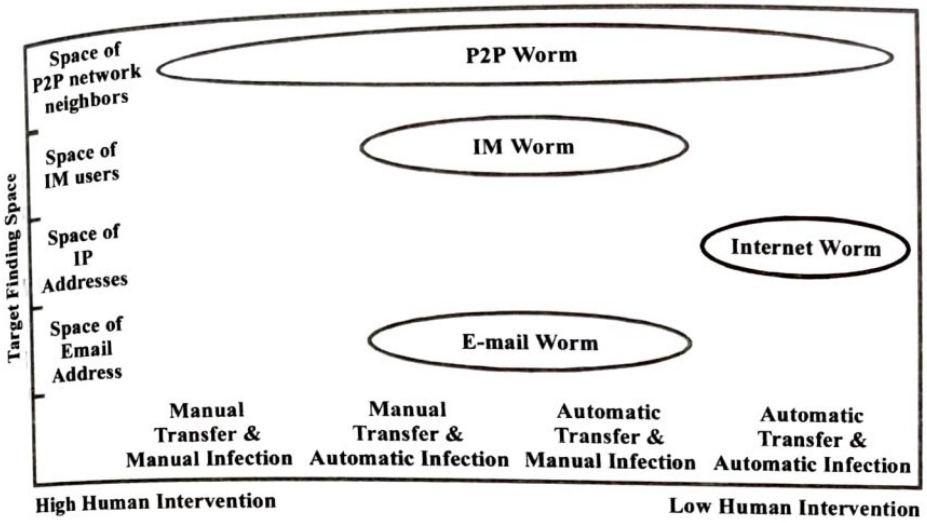


Fig. 5.3 Four Worm Classes

Q.23. What is the difference between viruses and worms ?

Ans. A *virus* and a *worm* are similar in that they're both forms of malicious software (*malware*). A virus infects another executable and uses this carrier program to spread itself. The virus code is injected into the previously benign program and is spread when the program is run. Examples of virus carrier programs are macros, games, e-mail attachments, Visual Basic scripts, games, and animations.

A worm is a type of virus, but it's self-replicating. A worm spreads from system to system automatically, but a virus needs another program in order to spread. Viruses and worms both execute without the knowledge or desire of the end user.

Q.24. Discuss the characteristics of a worm.

Ans. The various features of worms are as follows –

(i) Enhanced Targeting – The most important attribute of a worm is that it spreads its infection to other computers. But how does a worm know who to target next ?

Many target selection strategies have been proposed and implemented. Worms that spread through e-mail, for example, have an easy way to figure out their targets. All they need to do is look into their victim's mailbox or e-mail address book to find a set of targets. A mobile worm obtains phone numbers of its potential victims from the phone book in the cellphone hosting the worm. Some web worms use search engines to harvest URLs of potentially vulnerable targets.

Internet scanning worms, on the other hand, scan the IP address space for vulnerable machines. The most straightforward approach is ***random scanning*** – choosing IP addresses at random. This was adopted by Code Red Version-I. However, Code Red Version-II adopted ***localized scanning***. Over 80% of the time, it attempted to connect to victims with whom it shared the network address (most significant 8 or 16 bits of the IP address). This strategy was more successful since hosts in the same network are likely to be closer and be running the same software.

Worms like Nimda, unleashed in September 2001, spread aggressively thanks to its *five different vectors of propagation*. Propagation through HTTP and e-mail were particularly successful in penetrating the perimeter of the enterprise. Once inside, it exploited the Windows file-sharing feature to spread within the enterprise.

(ii) Enhanced Speed – To enhance the infection rate, some worms are designed to spawn *multiple threads*. Each thread is responsible for setting up connections to a different subset of hosts, thus increasing the rate at which infection is spread.

Some worms reduce infection latency by targeting a buffer overflow vulnerability on an application that employs UDP rather than TCP. TCP connection establishment involves a three-way handshake and is time-consuming. UDP, by contrast, is connectionless. This sharply reduces infection latency.

A steep increase in the number of infected machines at the very outset of a worm epidemic has a multiplicative effect on spreading rate. For this purpose, the attacker could create one or more ***bit-lists*** carrying addresses of several thousand vulnerable machines. The first worms to be let loose could carry one such list. As a worm infects each new machine, it splits its list between itself and the machine it has just infected. Given that most of the machines on the hit-lists are vulnerable, the worm spreads rapidly during the initial stage of the epidemic. Thereafter, the infected machines could spread the infection using random scanning or some other spreading method.

(iii) Enhanced Capabilities – Most worms (and viruses) have unique and distinct ***signatures*** – a pattern of bits, usually assembly language code, which appears in all instances of the worm. Worm and virus signatures are the key to detecting them. However, there are sophisticated code obfuscation techniques to evade detection. One such technique is the use of encryption for disguising worm code. Different instances of the worm may use different keys for encryption. Thus, they might fail to match any existing worm signatures. Such worms are said to be ***polymorphic.***

Some worms need to be *time-aware*. They obtain the current date and time from a network time protocol (NTP) server and can initiate specific actions at specified points of time. This capability allows worms to remain dormant for extended periods of time and then strike in a concerted fashion by, for example,

launching a denial of service attack at the same time. Some worms can *update themselves* by downloading code from given URLs. Alternatively, they may access a URL which in turn provides a set of URLs from which updated worm code may be downloaded. Finally, early e-mail worms used the host's e-mail services to spread infection while some more recent worms have been designed with a built-in SMTP engine which they use to send mail.

(iv) Enhanced Destructive Power – It is estimated that worms such as Code Red and Nimda caused ***billions of dollars in damage.*** How are these costs estimated ? Analysts estimate costs based on lost productivity, clean-up costs, and system downtime which affects business and revenues. Fast-spreading worms also caused severe network congestion problems disrupting normal Internet traffic and contributing to system down-time.

Nevertheless, most worms thus far have been relatively benign. Some worms contributed attack packets to a DDoS attack or caused Website defacement. The ***Witty*** worm which appeared in March 2004, however, was qualitatively different. It was the first worm to carry a destructive payload. It deleted a random section of the victim's hard disk leading to a system crash. It is not hard to imagine worms carrying for more destructive payloads that could crash many more systems.

The harm caused by a worm is not just destructive power measured by downtime, lost productivity, and system crashes. There are more sinister and subtle goals such as the stealing of sensitive personal and corporate information, which could remain undetected.

Q.25. What are the typical phases of operation of a virus or worm ?
(R.G.P.V., Dec. 2017)

Ans. During its operation, a typical virus goes through the following four phases –

(i) Dormant Phase – The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

(ii) Propagation Phase – The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

(iii) Triggering Phase – The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

(iv) Execution Phase – The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

A network worm exhibits the same characteristics as a computer virus – a dormant phase, a propagation phase, a triggering phase, and an execution phase. The propagation phase generally performs the following functions –

(i) Search for other systems to infect by examining host tables or similar repositories of remote system addresses.

(ii) Establish a connection with a remote system.

(iii) Copy itself to the remote system and cause the copy to be run.

The network worm may also attempt to determine whether a system has previously been infected before copying itself to the system. In a multiprogramming system, it may also disguise its presence by naming itself as a system process or using some other name that may not be noticed by a system operator.

As with viruses, network worms are difficult to counter. However, both network security and single-system security measures, if properly designed and implemented minimize the threat of worms

Q.26. Write short note on Trojan horse. (R.G.P.V., June 2008, Dec. 2015)

Or

Write short note on Trojans. ***(R.G.P.V., Dec. 2017)***

Ans. A Trojan is a malicious program disguised as something being. Trojans are often downloaded along with another program or software package. Once installed on a system, they can cause data theft and loss, and system crashes or slowdowns, they can also be used as launching points for other attacks such as Distributed Denial of Service (DDoS). Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts. Sophisticated Trojans can connect themselves to their originator or announce the Trojan infection on an Internet Relay Chat (IRC) channel. Table 5.1 lists some common Trojans and their default port numbers.

Table 5.1 Common Trojan Programs

Trojan	*Protocol*	*Port*
BackOrifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
Net Bus	TCP	12345 and 12346
Whack-a-mole	TCP	12361 and 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423 and 40426

Trojans ride on the backs of other programs and are usually installed on a system without the user's knowledge. A Trojan can be sent to a victim

system in many ways – as an Instant Messenger (IM) attachment, IRC an e-mail attachment, or NerBIOS file sharing. Many take programs supporting to the legitimate software such as freeware, spyware removal tools, system optimizers, screen savers, music, pictures, games and videos can install a Trojan on a system just by being downloaded.

Q.27. How does a Trojan work ?

Or

How Trojan horses affect the computer system/network ? ***(R.G.P.V., Nov. 2018)***

Ans. Trojans come in two parts, a Client part and a Server part. When the victim runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well. When the Server is being run on the victim's computer, it will (usually) try to hide somewhere on the computer, start listening on some port(s) for incoming connections from the attacker, modify the registry and/or use some other auto starting method.

It's necessary for the attacker to know the victim's IP address to connect to his/her machine. Many Trojans have features like mailing the victim's IP, as well as messaging the attacker via ICQ or IRC. This is used when the victim has dynamic IP which means every time you connect to the Internet you get a different IP (most of the dial-up users have this).

Most of the Trojans use Auto-Starting methods so even when you shut down your computer they're able to restart and again give the attacker access to your machine. New auto-starting methods and other tricks are discovered all the time. The variety starts from "joining" the Trojan into some executable file you use very often like explorer.exe, for example, and goes to the known methods like modifying the system files or the Windows Registry. System files are located in the Windows directory.

Q.28. List the different types of Trojans.

Ans. Trojans can be created and used to perform different attacks. Some of the most common types of Trojans are –

(i) Remote Access Trojans (RATs) – Used to gain remote access to a system.

(ii) Data-sending Trojans – Used to find data on a system and deliver data to a hacker.

(iii) Destructive Trojans – Used to delete or corrupt files on a system.

(iv) Denial of Service Trojans – Used to launch a denial or service attack.

(v) Proxy Trojans – This is a type of trojan horse designed to use the victim's computer as a proxy server. This gives the attacker an opportunity to do everything from your computer, including the possibility of conducting credit card fraud and other illegal activities, or even to use your system to launch malicious attacks against other networks.

(vi) FTP Trojans – Allows the attacker to use someone else's computer as an FTP server. Installing this Trojan onto your computer would enable the intruder to download/upload files from his PC to yours, which could provide another avenue more installation of malware.

(vii) Security Software Disabler Trojans – Used to stop antivirus software.

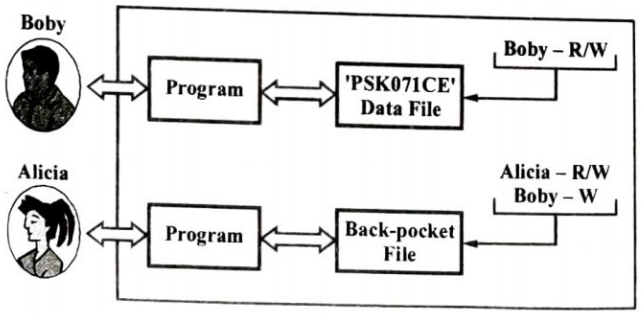
Q.29. Differentiate between proxy Trojans and FTP Trojans. ***(R.G.P.V., Dec. 2016)***

Ans. Refer to Q.28 (v) and (vi).

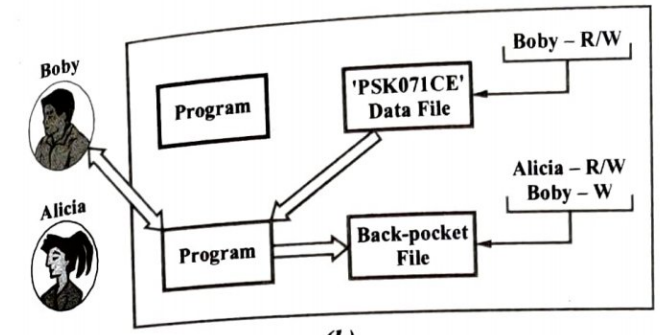
Q.30. In what ways a system can be defended from Trojan horse attack?

Ans. The use of a secure and trusted operating system can be one way to avoid Trojan horse attack. In the fig. 5.4, a Trojan horse is used to get around the standard security mechanism used by most operating systems and file management – the access control list. In this fig. 5.4, a user named Boby interacts using a program with a data file containing the critically sensitive character string 'PSK071CE'. This file is created by Boby with read/write permission provided to programs executing on his own behalf only.

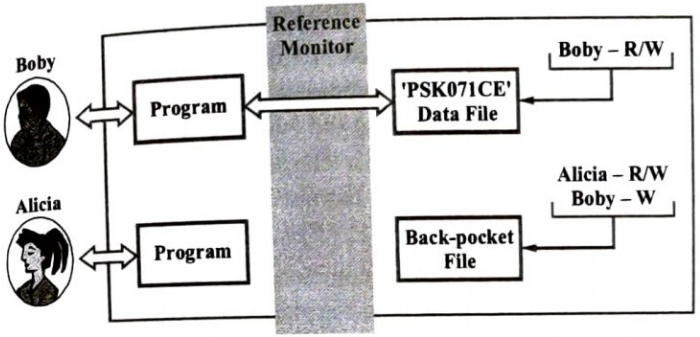
When a hostile user Alicia, gets legitimate access to the system and installs both a Trojan horse program and a private file to be used in the attack as a 'back pocket', Alicia gives only write permission to Boby and Read/Write permission to herself, as shown in fig. 5.4 (a). Now advertising it as useful utility, Alicia induces Boby to invoke the Trojan horse program. When it is detected that program is executed by Boby, it reads the sensitive character string from Boby's file and copies it into Alicia's back-pocket file as shown in fig. 5.4 (b).



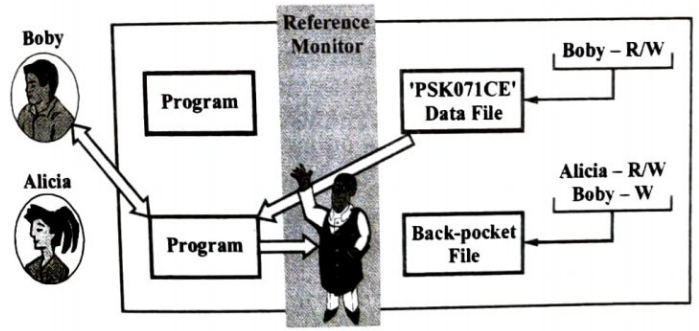
(a)



(b)



(c)



(d)

Fig. 5.4 Trojan Horse Defense

Now, as shown in fig. 5.4 (c), consider a secure operating system. The subjects are assigned security levels at logon, on the basis of criteria such as the terminal from which the computer is being accessed and the user involved, as identified by password/ID. In fig. 5.4 (c), there are two security levels, viz., sensitive and public, ordered in such a way that sensitive is higher than public. Now at sensitive security level processes owned by Boby and Boby's data file are assigned. Alicia's file and processes are restricted to public.

Now if a Trojan horse program is invoked by Boby [as shown in fig. 5.4 (d)], then the program acquires Boby's security level. So it is able to observe the sensitive character string, under the simple security property. When the program attempts to store the string in a public file (the back-pocket file), however, the *-property is violated and the attempt is disallowed by the reference monitor. Hence, the attempt to write into the back-pocket file is denied even though the access control list permits it. Hence, the security policy takes precedence over the access control list mechanism and thus system from Trojan horse attack is defended.

Q.31. Write short note on backdoors.
(R.G.P.V., Dec. 2010, June 2011, Dec. 2015, Nov. 2019)

Ans. A program or set of related programs that a hacker installs on a target system to allow access to the system at a later time, is known as ***backdoor.*** The goal of a backdoor is to remove the evidence of initial entry from the system's log files. A backdoor may also let a hacker retain access to a machine it has penetrated even if the intrusion has already been detected and remedied by the system administrator.

Adding a new service is the most common technique to disguise backdoors in the Window operating system. A hacker must investigate the system to find the services that are running on system, before the installation of a backdoor. The hacker could add a new service and give it an inconspicuous name or better yet choose a service that's never used and that is either activated manually or completely disabled.

This technique is effective because when a hacking attempt occurs the system administrator usually focuses on looking for something odd in the system, leaving all existing services unchecked. The backdoor technique is simple but efficient. The hacker can get back into the machine with the least amount of visibility in the server logs. In most cases, the backdoored services lets the hacker on higher privileges.

Remote Administration Trojans (RATs) are a class of backdoors used to enable remote control over a compromised machine. They provide apparently useful functions to the user, and at the same time, open a network port on the victim computer. Once the RAT is started, it behaves as an executable file, interacting with certain registry keys responsible for starting processes and sometimes creating its own system services. Unlike common backdoors, RATs hook themselves into the victim's operating system and always come packaged with two files – the client file and the server file. The server is installed in the infected machine, and the client is used by the intruder to control the compromised system.

Q.32. Write short note on logic bomb. ***(R.G.P.V., Nov. 2019)***

Ans. A logic bomb is a program, or portion of a program, which lies dormant until a specific piece of program logic is activated. In this way, a logic bomb is very analogous to a real-world land mine. The most common activator for a logic bomb is a date. The logic bomb checks the system date and does nothing until a pre-programmed date and time is reached. At that point, the logic bomb activates and executes its code. The most dangerous form of the logic bomb is a logic bomb that activates when something doesn't happen. Because a logic bomb does not replicate itself, it is very easy to write a logic bomb program. This also means that a logic bomb will not spread to unintended victims. In some ways, a logic bomb is the most civilized programmed threat, because a logic bomb must be largeted against a specific victim.

Q.33. Write short note on firewalls. ***(R.G.P.V., Nov. 2019)***

Ans. Conceptually, a firewall can be compared with a sentry standing outside an important person's house i.e., such as the nation's president. This sentry keeps an eye on and physically checks every person that enters into or comes out of the house. If the sentry senses that a person wishing to enter the president's house is carrying a knife, the sentry would not allow the person to enter. Similarly, even if the person does not possess any restricted objects, but somehow looks suspicious, the sentry can prevent that person's entry.

A firewall acts like a sentry. If implemented, it guards a corporate network by standing between the network and the outside world. All traffic between the network and the Internet in either direction must pass through the firewall. The firewall decides if the traffic can be allowed to flow, or whether it must be stopped from proceeding further. This is illustrated in fig. 5.5.

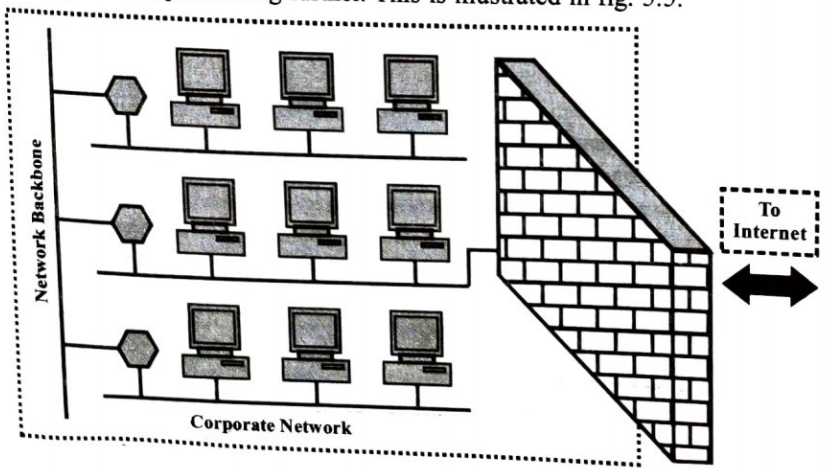


Fig. 5.5 A Firewall

Of course, technically, a firewall is a specialized version of a router. In addition to the basic routing functions and rules, a router can be configured to perform the firewall functionality, with the help of additional software resources.

The characteristics of a good firewall implementation can be described as follows –

(i) All traffic from inside to outside, and vice versa, must pass through the firewall. This can be achieved if all the access to the local network must first be physically blocked and access only through the firewall should be permitted.

(ii) Only the traffic authorized by the local security policy should be allowed to pass through.

(iii) The firewall itself must be strong enough, so that to render attacks on it useless.

DoS AND DDoS ATTACKS, BUFFER OVERFLOW, ATTACK ON WIRELESS NETWORKS, PHISHING – METHOD OF PHISHING, PHISHING TECHNIQUES

Q.34. Write short note on DoS attack. ***(R.G.P.V., Dec. 2017)***

Ans. The attacks in which an attacker prevents legitimate users from accessing the services for which he is authorized, by flooding the bandwidth of a network or by filling his/her e-mail box by spams. But it does not allow any unauthorized access to the services or network of legitimate user. This type of attacker don't want to access the services of legitimate users, they have only destructive mindset. In DoS the attacker only want to destroy or hang the services or network of user. Since the motive of attackers for carrying out these types of attacks, is not definite. Either they want to slow down a network or they want to destroy the network completely for creating problems to users. The attackers in this type of attack mainly focus on the computers which are connected to the Internet.

The messages were sent repeatedly to the victim machine in earliest type of DoS attacks. Since most machines at that time had resources that could be depleted easily, so machines were vulnerable to these attacks. It was common for the attacker to send mails or malicious packets from fake source addresses so that they cannot be caught. So these attackers and packets were difficult to recognize from malicious machines, to filter them at a firewall.

Now attackers are focusing on websites or services which are hosted on a high-profile web servers like online shopping sites, bank, online and debit card paymet systems etc. To apply this type of attack, buffer overflow technique

is used, which is also known as spoofing. In buffer overflow technique the attacker fills the network of victim's machine with continuous request. Since in spoofing the IP address of attacker is fake so the victim's machine wait to response these requests. The bandwidth of the network then consumed and the network fails to respond the requests which are not fake and the network finally breaks down.

Following are some signs of DoS attacks which was given by the United States Computer Emergency Response Team –

(i) When the users try to open a file or access a website then it takes more time than it should take. It means that the performance of network is slow.

(ii) When we want to access a website and the website is unavailable.

(iii) When the users get unexpected e-mails or spams then it is also significance of DoS attack.

Q.35. Briefly discuss the various types of DoS attacks.

Ans. Some of the DoS attacks are as follows –

(i) IP Spoofing – IP spoofing is forging of an IP packet address. In particular, a source address in the IP packet is forged. Since network routers use packet destination address to route packets in the network, the only time a source address is used is by the destination host to respond back to the source host. So forging the source IP address causes the responses to be misdirected, thus creating problems in the network. Many network attacks are a result of IP spoofing.

(ii) Smurf Attack – In this attack, the intruder sends a large number of spoofed ICMP Echo requests to broadcast IP addresses. Hosts on the broadcast multicast IP network, say, respond to these bogus requests with reply ICMP Echo. This may significantly multiply the reply ICMP Echos to the hosts with spoofed addresses.

(iii) Buffer Overflow Attack – In this attack, the attacker floods a carefully chosen field such as an address field with more characters than it can accomodate. These excessive characters, in malicious cases, are actually executable code, which the attacker can execute to cause havoc in the system, effectively giving the attacker control of the system. Since anyone with little knowledge of the system can use this type of attack, buffer overflow has become one of the most serious classes of security threats.

(iv) Ping of Death Attack – This vulnerability is used to hang remote systems so that no user could use its services. A system attacker sends IP packets that are larger than the 65,536 bytes allowed by the IP protocol. Many operating systems, including network operating systems, cannot handle these oversized packets, so they freeze and eventually crash.

(v) Teardrop Attack – The teardrop attack uses a program that causes fragmentation of a TCP packet. It exploits a reassembly and causes the victim system to crash or hang.

(vi) SYN Attack – The SYN attack exploits TCP/IPs three-way handshake. In a normal three-way handshake, the client sends a SYN packet to the host, the host replies to this packet with a SYN ACK packet. Then the client responds with a TCP ACK (acknowledgement).

Now, in a SYN attack too, several SYN packets are sent to the server but all these SYN packets have a bad source IP address. When the target systems receives these SYN packets with bad IP addresses, it tries to respond to each one of them with a SYN ACK packet. Now, the target system waits for a ACK message to come from the bad IP address. It queues up all these requests until it receives an ACK message. The requests are not removed unless and until the remote target system gets an ACK message. Hence, these requests take up or occupy valuable resources of the target machine.

To actually effect the target system, a large number of SYN bad IP packets have to be sent. Since these packets have a bad source IP, they queue up, use up resources and memory or the target system and eventually crash, hang or reboot the system.

A land attack is same as a SYN attack, the only difference being that instead of a bad IP address, the IP address of the target system is used.

(vii) SYN Flooding – A three-way handshake used by the TCP protocols to initiate a connection between two network elements. During the handshake, the port door is left half open. A SYN flooding attack is flooding the target system with so many connection requests coming from the spoofed source addresses that the victim server cannot complete because of the bogus source addresses. In the process all its memory gets hogged up and the victim is thus overwhelmed by these requests and can be brought down.

(viii) Sequence Number Sniffing – In this attack, the intruder takes advantage of the predictability of sequence numbers used in TCP implementations. The attacker then uses a sniffed text sequence number to establish legitimacy.

Q.36. What are DoS attacks ? Discuss any three classified DoS attacks in brief. ***(R.G.P.V., Dec. 2010, June 2011)***

Or

What do you mean by denial of service ? Write various denial of service attacks. Explain any two. ***(R.G.P.V., Dec. 2013)***

Ans. **DoS Attacks** – Refer to Q.34.

Types of DoS Attacks – Refer to Q.35.

Q.37. Discuss the various tools used for DoS attack.

Ans. There are many tools that use different type of traffic so that a victim's computer can be flooded. But the motive of attacker is same. Since there are large number of requests sent by attacker, which are waiting for response, so the services on system or all the system is unavailable to user. Although in DoS attack, the attacker does not want to access the system or network so it is an unsophisticated attack, therefore it is called the attack of last resort. Here the attacker only harms the victim's machine or interrupts the victim's machine.

Some tools are given below, which launch the DoS attack –

(i) Targa – Targa is a very interesting tool to launch a DoS attack. It is capable of running eight different DoS attacks. Using this tool the attackers are capable to launch an individual attack or any set of attacks until it get success.

(ii) Nemesy – By using this tool, the attackers are enabled to generate random packets of spoofed address.

(iii)Jolt2 – This type of tool is used to attack on window's based networking code. This tool enables attacker to attack on window based machines and this attack causes the 100% consumption of CPU time on processing of illegal packet.

(iv) Some Trouble – This tool is also a remote tool. It floods the network, so this is called remote flooder or remote bomber.

(v) Crazy Pinger – If an attacker is targetting the whole network then this tool can be used. Using this tool attacker is enable to send large packets of ICMP to a remotely targetted network.

Q.38. How can the DoS attacks be prevented ?

Ans. There are many preventing measures of DoS attacks, some of them are as follows –

(i) Router filters should be implemented time-to-time. It will reduce the risk of certain DoS attacks.

(ii) A baseline should be established for ordinary activities. This baseline should be used to observe system's performance, disk usage, CPU usage or network activity etc.

(iii) As our current needs, we should check our physical security aspects time-to-time.

(iv) We should install a fault-tolerant network.

(v) Regular backup schedules should be established and maintained.

(vi) Password policies to access highly privileged accounts like Unix root and Microsoft Windows NT administrator should be established and maintained properly.

(vii) If there are unused and unessential services on our system, which cause the attacker to take advantage of these services to execute DoS, then should uninstall that services.

(viii) Patches can be installed to avoid TCP SYN flooding.

Q.39. What are DDoS attacks ? Explain. Also discuss the tools used in DDoS attack.

Ans. DDoS is also known as distributed denial of service attack. In this type of attack an attacker may use one computer to attack on another computer. An attacker can take control of your computer by using security vulnerabilities or security weaknesses of system. Now once taking control over computer he/she enforce the computer to send a vast amount of data over network or to a website. Since the attacker is using multiple computers to launch the DoS attack so the attack is distributed.

In DDoS a large number of zombie systems are synchronized for attacking on a system. Here main target, to which attacks are applied is called "primary victim" and the zombie systems which are attacking are known as "secondary victim".

Usually denial of service attack mechanism is launched on specific date and time. DDoS attack mechanism can also be applied by malware, MyDoom is the example of this. Prior to release of the malware the DDoS attacks includes hardcoding the data forget, therefore to launch the attack no further instruction is needed. An attacker can also download a zombie agent, when a Trojan is included in the system. Now to launch a DoS/DDoS attack, the Botnet is the popular medium.

Tool used to launch DDoS attacks are as follows –

(i) Tribe Flood Network (TFN) – Tribe flood network is a tool, which includes the set of programs to launch different DDoS attacks such as ICMP, flood, SYN flood, UDP flood etc.

(ii) Stacheldraht – It acts as DDoS agent and is randomly written for linux and solaris operating system.

(iii) Trinoo – Trinoo systems are believed to be set on thousands of systems on the Internet that have been compromised by remote buffer overrun exploit. It is a set of computer programs.

(iv) Shaft – In this tool client controls the size of flooding packets and duration of the attack, though it is packet flooding attack. It is conceptually like a Trinoo.

(v) MStream – In this tool communication is performed through TCP and UDP packets. Spoofed TCP packet with ACK flag set to attack the target are used in this tool. Here packet handler accessing is password protected.

This tool has a unique feature that other DDoS tool don't have. All the connected users of access successful or not, to the handler(s) are informed by this tool.

Q.40. Write short note on DDoS. ***(R.G.P.V., Dec. 2011)***

Ans. Refer to Q.39.

Q.41. How DoS and DDoS attacks can be performed ? ***(R.G.P.V., Nov. 2018)***

Ans. **DoS Attack** – Refer to Q.34.

DDoS Attack – Refer to Q.39.

Q.42. What is DDoS ? Describe the 3 lines of defence against DDoS attacks. ***(R.G.P.V., Dec. 2012)***

Ans. **DDoS** – Refer to Q.39.

Defence Against DDoS Attacks – Three lines of defence against DDoS attacks are as follows –

(i) Attack Prevention and Prevention (Before the Attack) – These mechanisms allow the victim to endure attack attempts without denying service to legitimate clients. Techniques include enforcing policies for resource consumption and providing backup resources as required. Besides, prevention mechanisms modify systems and protocols on the Internet to minimize the chances of DDoS attacks.

(ii) Attack Detection and filtering (During the Attack) – These mechanisms tries to find the attack as starts and respond immediately. This reduces the effect of the attack on the target. Detection involves looking for suspicious patterns of behaviour. Response involves filtering out packets likely to be part of the attacks.

(iii) Attack Source Traceback and Identification (During and After the Attack) – This is an attempt to recognize the source of the attack as a first step in preventing future attacks. Although, this method does not yield results fast enough, if at all, to mitigate an ongoing attack.

Q.43. What do you mean by buffer overflow ? Explain.

Ans. Data stored by a process, in a buffer outside the memory without intervention of a program, is known as buffer overflow. In this attack the adjacent memory is overwritten by the extra data, which may contain other data, including program variables and program flow control data. The result of data overflow may be erratic program behaviour, including memory access errors, incorrect results, program termination etc.

The inputs that are designed to execute a code or altering the way the program operates, can trigger the buffer overflow. Buffer overflow can be prevented by bounds checking.

C and C++ are common programming languages which are associated with buffer overflows because there is no built-in protection against overwriting data in any part of memory or accessing data and there is no automatic check mechanism that the data written to an array is within the boundaries of that array.

When it is tried to store more data in a buffer than it can hold, by a program or process, then buffer overflow occurs. Since buffers can contain limited amount of data, the extra data – which has to go somewhere – can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Buffer overflow is a common type of security attack on data integrity.

We should have the knowledge of any high-level computer language such as C, C++ or any other, because basic knowledge of process memory layout is important. There is no automatic bounds checking in C and C++, a user can

write a buffer like –

```
void main( )
{
    int a[20];
    a[30] = 20;
}
```

Q.44. Explain the various types of buffer overflow.

Ans. Types of buffer overflow are as follows –

(i) Stack-based Buffer Overflow – When on program's call a program writes to a memory address, outside the intended data structure usually a fixed length buffer, then stack buffer overflow occurs. The characteristics of stack based programming are –

(a) The memory space in which automatic variables are allocated is known as stack.

(b) Usually function parameters have garbage until they are initialized because they are allocated on the stack and not automatically initialized by the system.

(c) The reference to the variable in stack is removed on the completion of function cycle.

To manipulate the program in various ways the attacker may exploit stack-based buffer overflows by overwriting –

(a) A local variable may benefit the attacker, that is near the buffer in memory on the stack.

(b) Execution will resume at the return address as specified by the attacker, once the function returns.

(c) A function pointer which is to be executed.

(ii) NOPs – An assembly language instruction/command that does nothing is called no operation (NOP) or no operation performed (NOOP). State of status flags or memory locations in the code are not changed using this command. By using NOP the developer can force memory alignment to act as a place holder and later on to be replaced by an active instruction in program development.

When the exact value of the instruction pointer is indeterminate, the NOP slide which was created by NOP opcode, allows code to execute. By increasing the size of target stack buffer area the NOP help to know/locate the exact address of buffer. The attackers can bad their code with NOP code to increase the chance of finding the exact memory address. If it is done then a larger section of stack is corrupted with the NOP machine instruction. After the NOP instructions, an instruction is placed to perform a relative jump to the top of the buffer where the shellcode (A shellcode is a small piece of code used as a payload in the exploitation of software vulnerability) is located, at the end of attacker's supplied data.

(iii) Heap Buffer Overflow – Heap buffer overflow may be introduced accidentally by an application programmer and it is occurred in the heap data area. When an application copies more data into a buffer than the buffer designed to contain, then the buffer overflow occurred. A routine, which is not verifying that the source will fit into the destination or not, while copying data into a buffer, is vulnerable to exploit.

The characteristics of heap-based programming are –

(a) In a heap dynamic objects are allocated because it is a memory space.

(b) The functions allocated dynamically new( ), calloc( ) and malloc( ) in the heap use space in memory which is allocated by heap.

(c) The variables which are declared dynamically are declared on the heap before execution.

Memory allocated by the application at run-time on the heap is dynamic and normally contains program data.

Q.45. Write down the techniques to minimize the buffer overflow.

Ans. Since all the attacks cannot be prevented but there are some techniques which can reduce these attacks –

(i) Assessment of Secure Code – We have read that when any application tries to copy more data than it was designed to hold, then buffer overflow occurs. Programmers should have the knowledge to minimize the use of vulnerable C functions available in library, such as strcpy( ), strcat( ), sprintf( ), etc. which operate on null-terminated strings and perform no bounds checking.

(ii) Disable Stack Execution – Malicious code which reside in the stack, causes input argument to the program, it does not reside in the code segment. A segmentation violation will be caused when any code attempts to execute the other code residing in the stack. The solution of this problem is to invalidate the stack to execute any instructions. However, the solution is not easy to implement, although it is possible in Linux. Trampoline functions are used by some compilers to implement taking the address of a nested function that works on the system stack being executable. A trampoline is a small piece of code created at run-time when the address of a nested function is taken. Trampoline requires the stack to be executable, since it resides in the stack and in the stack frame of the containing function.

(iii) Compiler Tools – Since the compilers have become more powerful in optimization and the checks they perform, over the years, so they offer warnings on the use of unsafe constructs such as gets( ), strcpy( ), etc. If such warnings are displayed, then programmers should be adviced to restructure the code.

(iv) Dynamic Run-time Checks – In this method, to prevent attacks, an application has restricted access. In this scheme a preloaded safety code is executed before an application. A safer version of unsafe standard function can be provided by this preloaded code or it can be ensured by it, that no return addresses are overwritten.

Q.46. What are wireless network attacks ? Explain the various techniques of attacks on wireless networks.

Ans. If anyone is talking about the wired and wireless networks, then he wants to focus on one thing in both networks i.e., trust (security). Hardware on a wired network are directly under control of administrator and therefore wired networks are assumed to be one of the trust. While in a wireless network someone could sit around the network with a laptop and can access the wireless network. Therefore wireless workstations are assumed to be one of the distrust. On the basis of this the administrators focus on both network some when it comes to guarding network security. Although they extremely focus on wireless networks in compare to wired network.

The unauthorized access of wireless network by penetrating its security is known as wireless cracking. The cracking of WLANs demand less technological skills. There are various techniques to attack on wireless networks. Some of them are as follows –

(i) Sniffing – It is the simplest attack among all attacks. The wireless data which is being broadcasted on an unsecured network can be easily intercepted using sniffing. The information about the active/available Wi-Fi networks gathered by a technique called reconnaissance. The sniffers are remotely installed on victim's system and such activities are conducted –

(a) Scanning of wireless networks
(b) Detection of SSID
(c) Collection of MAC address
(d) Collection of frames to crack WEP.

(ii) Spoofing – The main objective of this attack is to gain an illegal advantage by changing/modifying the identity of legitimate user by falsifying his/her data. The attacker simply create a new network with strong signals and often launches an attack on a wireless network by copying a SSID in the same manner as legitimate network. By doing so computers are connected to spoofed network instead of real. The computers need not to be informed to access the network while a wireless network is installed because as soon as they move within signal range they automatically access it, so the attackers can conduct this activity easily.

Different types of spoofing are as follows –

(a) MAC Address Spoofing – Changing of an assigned media access control (MAC) address of a networked device to another one, is known as MAC address spoofing. In this type of spoofing attackers can bypass the access control lists on servers or routers by either hiding a computer on a network or allowing it to impersonate another network device.

(b) IP Spoofing – The process of creating IP packets with a forged source IP address, so that identity of the sender is concealled, is known as IP spoofing. In this, a variety of techniques is used to find an IP address that is of trusted host. Now attacker modifies the packet headers so that it looks like that the packets are coming from the host that is legitimate.

(c) Frame Spoofing – The frames valid as per 802.11 standard and whose content is spoofed carefully are injected by the attacker. Frames having spoofed source address, cannot be detected easily unless the address is entirely faked/bogus, because they are not authenticated in 802.11 networks themselves.

(iii) Main-in-the Middle Attack (MITM) – The motive of this attack is to observe the communication between two hosts or modify it. In this attack, the attacker on host S, inserts S between all communications between the hosts P and Q without the knowledge of P and Q. Hence all messages sent by P reaches Q but via S and vice versa.

(iv) Encryption Cracking – The primary step to protect wireless networks is to use WPA encryption. New tools and techniques are always devised by attackers to deconstruct older encryption technology, which is quite easy for attackers due to continuous research in this field. Now second and important step is to use a long and randomized key, because these keys are much harder to crack.

Q.47. How can a wireless network be secured ? Explain.

Ans. The security features of wireless networks are still ignored, especially, by home users, however now they are not time-consuming and non-intuitive. The strength and security of a wireless network can be improved by following steps –

(i) Enable your device with WPA/WEP encryption.
(ii) Default SSID should be changed.
(iii) The default settings of all the equipments/components of wireless networks should be changed.
(iv) Filtering of MAC address should be enabled.
(v) SSID of a wireless network should not be broadcasted.
(vi) Remote login should be disabled.
(vii) The names which can be easily identified should not be provided to the network.
(viii) We should connect our system only to secured wireless network.
(ix) Firmware of a router should be upgraded regularly.

There are some tools that can also be used to secure a wireless network.

(i) AirDefense Guard – It is based on signature analysis and advanced intrusion detection for wireless LANs is provided by this tool. It is also based on policy deviation, protocol assessment policy deviation and statistically anomalous behaviour.

(ii) Google Secure Access – The Internet traffic is encrypted by Google secure and sent through Google's servers on the Internet. Anyone can go online for free by accessing the network name "Google Wi-Fi", which is secured by Google's VPN, with your Wi-Fi enabled device and a Google Account.

(iii) Zamzom Wireless Network Tool – It is a freeware tool which maintain computer security, detects all computer names, Mac and IP addresses

utilizing a single wireless network and helps to protect a wireless network. It reveals all computers both authorized and unauthorized – who have access over the wireless network.

Q.48. Discuss the phishing. ***(R.G.P.V., Dec. 2012)***

Or

Explain the term phishing in detail. ***(R.G.P.V., Nov. 2019)***

Ans. Phishing, in its most common form, is the process of *luring* a victim to a *fake Website* by clicking on a link. The victim usually encounters the link in an e-mail message sent to him or on a Webpage being browsed by him as in the following examples –

(i) Click here www.luckyDraw.com to claim your $1,000,000 prize!

(ii) *Urgent attention of all TrueBank Account Holders.*

Following a security breach, we wish to inform all our existing customers that we need to verify their account details. Kindly click here

www.Truebank.com

to proceed.

(iii) The ultimate experience with the hottest babes in town.

Click here for further details

www.HotBabesAndHunks.com

Once the victim clicks on the link such as that shown in fig. 5.6, he/she may be induced to *divulge sensitive information* such as his credit card number or a password. For example, one of the highly publicized scams in recent times has been the phishing attacks on *on-line banks*.

TrueBank™

Dear customer

This is to confirm that you have recently attempted to withdraw Rs.5000 from your checking account while in another country.

In case this information is incorrect, it is possible someone may have gained access to your account. To ensure safety of your account please visit our Website via the link given below to verify your personal information.

http//www.TruBank.com/customers/verifyinfo.asp

We require your immediate cooperation to rectify this discrepancy.

Thank you,
TrueBank

Fig. 5.6 An Example of a Phishing Attempt

Phishing attempts often use URLs that are very similar to the real URL. For example, the real URL may be www.TrueBank.com but the fake one may

be www.TruBank.com. The fake URL corresponds to a Website owned and operated by the attacker. Once the user clicks on the fake link, he/she is presented with a Web page that has the same look and feel as that of the original Website. He/she is then asked to enter his/her login name and password. So as not to arouse any suspicion, he/she may be directed to the true site after entering his/her password. But, by then, the attacker has harvested sensitive information like his/her password.

Q.49. Discuss the different methods of phishing.

Ans. Three of the most popular methods phishers employ are as follows –

(i) Impersonation – Impersonation is the most popular and the most simple method of deceit. It consists of a completely constructed fake site that the recipient is deceived into visiting. This fake site contains images from the real Web site and might even be linked to the real site.

(ii) Forwarding – Forwarding is seen more with Amazon, eBay, and PayPal and is an e-mail you typically receive that has all the usual real Web site graphics and logins within it. When a victim logs in via a Forwarding e-mail link, the user's data is sent to the hostile server, then the user is forwarded to the real site, and in many cases, the system logs you into the real site via a man-in-the-middle (MITM) technique. This Forwarding attack continuity is flawless, and victims usually never know that they were phished. The weakness with this approach is that it relies on the spam itself to get through without being filtered. Due to the amount of HTML within such an e-mail, many corporate antivirus and antispam filters will block it because the Bayesian points rise with more encapsulated HTML.

(iii) Popups – The third basic method is the popup attack, a very creative but limited approach. The popup technique was first discovered during the barrage of phishing attacks on Citibank in September 2003. This was essentially a link that you clicked within your e-mail, and it posted a hostile popup. But behind the popup was the actual target that the attackers were trying to steal data from. This is quite a slick, creative ploy that is actually one of the most authentic looking of the three basic phishing methods. However, popup attacks are very ineffective today, since most browsers now have popup blockers installed by default (Mozilla/FireFox and Service Pack 2 for XP).

Q.50. Explain the different types of phishing. ***(R.G.P.V., Nov. 2018)***

Ans. Numerous different types of phishing attacks have now been identified. Some of the more prevalent are listed below –

(i) Man-in-the-Middle Phishing – It is harder to detect than many other forms of phishing. In these attacks hackers position themselves between the user and the legitimate Website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.

(ii) URL Obfuscation Attacks – The secret for many phishing attacks is to get the message recipient to follow a hyperlink (URL) to the attacker's server, without them realising that they have been duped. Unfortunately phishers have access to an increasingly large arsenal of methods for obfuscating the final destination of the customer's web request.

The most common methods of URL obfuscation are –

(a) Bad Domain Names – One of the most trivial obfuscation methods is through the purposeful registration and use of bad domain names. Consider the financial institute MyBank with the registered domain mybank.com and the associated customer transactional site http://privatebanking.mybank.com. The phisher could set up a server using any of the following names to help obfuscate the real destination host –

(1) http://privatebanking.mybank.com.**ch**
(2) http://mybank.**privatebanking**.com
(3) http://privatebanking.**mybonk**.com or even http://privatebanking.**mybank**.com
(4) http://privatebanking.mybank.**hackproof.com**

It is important to note that as domain registration organizations move to internationalize their services, it is possible to register domain names in other languages and their specific character sets. For example, the Cyrillic "o" looks identical to the standard ASCII "o" but can be used for different domain registration purposes - as pointed out by a company who registered microsoft.com in Russia a few years ago.

Finally, it is worth noting that even the standard ASCII character set allows for ambiguities such as upper-case "i" and lower-case "L".

(b) Friendly Login URL's – Many common web browser implementations allow for complex URL's that can include authentication information such as a login name and password. In general the format is URL://**username:password@hostname**/path.

Phishers may substitute the username and password fields for details associated with the target organization. For example the following URL sets the *username = mybank.com, password = ebanking* and the destination hostname is *evilsite.com.*

http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm

This friendly login URL can successfully trick many customers into thinking that they are actually visiting the legitimate MyBank page. Because of its success, many current browser versions have dropped support for this URL encoding method.

(c) Third-party Shortened URL's – Due to the length and complexity of many Web based application URLs – combined with the way URL's may be represented and displayed within various e-mail systems (e.g., extra spaces and line feeds into the URL) – third-party organizations have sprung up offering free services designed to provide shorter URL's.

Through a combination of social engineering and deliberately broken longs or incorrect URL's, Phishers may use these free services to obfuscate the true destination. Common free services include **http://smallurl.com** and **http://tinyurl.com**.

(d) Host Name Obfuscation – Most Internet users are familiar with navigating to sites and services using fully qualified domain name, such as www.evilsite.com. For a Web browser to communicate over the Internet, this address must to be resolved to an IP address, such as 209.134.161.35 for www.evilsite.com. This resolution of IP address to host name is achieved through domain name servers. A Phisher may wish to use the IP address as part of a URL to obfuscate the host and possibly bypass content filtering systems, or hide the destination from the end user.

For example the following URL –

http://mybank.com:ebanking@evilsite.com/phishing/fakepage.htm

(1) Octal-address expressed in base 8
(2) Hexadecimal-address expressed in base 16.

These alternative formats are best explained using an example. Consider the URL http://www.evilsite.com/, resolving to 210.134.161.35. This can be interpreted as –

(1) Decimal – http://210.134.161.35/
(2) Dword – http://3532038435/
(3) Octal – http://0322.0206.0241.0043/
(4) Hexadecimal – http://0xD2.0x86.0xA1.0x23/ or even http://0xD286A123/
(5) In some cases, it may be possible to mix formats (e.g., http://0322.0x86.161.0043/)

(e) URL Obfuscation – To ensure support for local languages in Internet software such as Web browsers and e-mail clients, most software will support alternate encoding systems for data. It is a trivial exercise for a Phisher to obfuscate the true nature of a supplied URL using one (or a mix) of these encoding schemes.

These encoding schemes tend to be supported by most Web browsers, and can be interpreted in different ways by Web servers and their custom applications. Typical encoding schemes are –

(1) Escape Encoding – Escaped-encoding, or sometimes referred to as percent-encoding, is the accepted method of representing characters within a URL that may need special syntax handling to be correctly interpreted. This is achieved by encoding the character to be interpreted with a sequence of three characters. This triplet sequence consists of the percentage character "%" followed by the two hexadecimal digits representing the octet code of the original character. For example, the US-ASCII character set represents a space with octet code 32, or hexadecimal 20. Thus its URL-encoded representation is %20.

(2) Unicode Encoding – Unicode encoding is a method of referencing and storing characters with multiple bytes by providing a unique reference number for every character no matter what the language or platform. It is designed to allow a Universal Character Set (UCS) to encompass most of the world's writing systems. Many modern communication standards (such as XML, Java, LDAP, JavaScript, WML, etc.), operating systems and Web clients/

servers use Unicode character values. Unicode (UCS-2 ISO 10646) is a 16-bit character encoding that contains all of the characters (216 = 65,536 different characters total) in common use in the world's major languages. Microsoft Windows platforms allow for encoding of Unicode characters in the following format –%u0000 – for example %u0020 represents a space, while %u01FC represents the accented AE and %uFD3F is an ornate right parenthesis.

(3) Inappropriate UTF-8 Encoding – One of the most commonly utilised formats, Unicode UTF-8, has the characteristic of preserving the full US-ASCII character range. This great flexibility provides many opportunities for disguising standard characters in longer escape-encoded sequences. For example, the full stop character "." may be represented as %2E, or %C0%AE, or %E0%80%AE, or %F0%80%80%AE, or %F8%80% 80% 80%AE, or even %FX%80%80%80%80%AE.

(4) Multiple Encoding – Various guidelines and RFC's carefully explain the method of decoding escape encoded characters and hint at the dangers associated with decoding multiple times and at multiple layers of an application. However, many applications still incorrectly parse escape-encoded data multiple times.

Consequently, phishers may further obfuscate the URL information by encoding characters multiple times (and in different fashions). For example, the back-slash "\" character may be encoded as %25 originally, but could be extended to – % 255C, or %35C,or %%35%63, or %25%35%63, etc.

(iii) Hidden Attacks – Extending beyond the obfuscation techniques discussed earlier, an attacker may make use of HTML, DHTML and other scriptable code that can be interpreted by the customers Web browser and used to manipulate the display of the rendered information. In many instances the attacker will use these techniques to disguise fake content (in particular the source of the page content) as coming from the real site – whether this is a man-in-the-middle attack, or a fake copy of the site hosted on the attackers own systems.

The most common vectors are –

(a) Hidden Frames – Frames are a popular method of hiding attack content due to their uniform browser support and easy coding style.

In the following example, two frames are defined. The first frame contains the legitimate site URL information, while the second frame – occupying 0% of the browser interface – references the phishers chosen content. The page linked to within the hidden frame can be used to deliver additional content (e.g., overriding page content or graphical substitution), retrieving confidential information such as SessionID's or something more nefarious; such as executing screen-grabbing and key-logging observation code.

```
<frameset rows="100%, *" framespacing="0">
<frame name="real" src="http://mybank.com/" scrolling="auto">
<frame name="hiddenContent" src="http://evilsite.com/bad.htm"
scrolling = "auto"
</frameset>
```


(b) Overriding Page Content – Several methods exist for phishers to override displayed content. One of the most popular methods of inserting fake content within a page is to use the DHTML function - DIV. The DIV function allows an attacker to place content into a "virtual container" that, when given an absolute position and size through the STYLE method, can be positioned to hide or replace (by "sitting on top") underlying content. This malicious content may be delivered as a very long URL or by referencing a stored script. For example, the following code segment contains the first three lines of a small JavaScript file (e.g., fake.js) for overwriting a pages content.

```
var d = document;
d.write('<DIV id="fake" style="position:absolute; left:200; top:200; z-
index:2">
<TABLE width=500 height=1000 cellspacing=0 cellpadding=14><TR>');
d.write('<TD colspan=2 bgcolor=#FFFFFF valign=top height=125>');
.....
```

This method allows an attacker to build a complete page (including graphics and auxiliary scripting code elements) on top of the real page.

(c) Graphical Substitution – While it is possible to overwrite page content easily through multiple methods, one problem facing phishers is that of browser specific visual clues to the source of an attack. These clues include the URL presented within the browsers URL field, the secure padlock representing an HTTPS encrypted connection, and the Zone of the page source. A common method used to overcome these visual clues is through the use of browser scripting languages (such as JavaScript, VBScript and Java) to position specially created graphics over these key areas with fake information.

(iv) Client-side Vulnerabilities – The sophisticated browsers customers use to surf the web, just like any other commercial piece of software, are often vulnerable to a myriad of attacks. The more functionality built into the browser, the more likely their exists a vulnerability that could be exploited by an attacker to gain access to, or otherwise observe, confidential information of the customer.

While software vendors have made great strides in methods of rolling out software updates and patches, home users are notoriously poor in applying them. This, combined with the ability to install add-ons (such as Flash, RealPlayer and other embedded applications) means that there are many opportunities for attack.

Similar to the threat posed by some of the nastier viruses and automated worms, these vulnerabilities can be exploited in a number of ways. However, unlike worms and viruses, many of the attacks cannot be stopped by anti-virus software as they are often much harder to detect and consequently prevent (i.e., the stage in which the antivirus product is triggered, is usually after the exploitation and typically only if the attacker tries to install a well known Backdoor Trojan or Key-logger utility).

(v) ***Deceptive Phishing*** – The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method today is a deceptive e-mail message. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.

(vi) ***Malware-based Phishing*** – It refers to scams that involve running malicious software on users' PCs. Malware can be introduced as an e-mail attachment, as a downloadable file from a Web site, or by exploiting known security vulnerabilities – a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up-to-date.

(vii) ***DNS-Based Phishing ("Pharming")*** – Pharming is the term given to hosts file modification or Domain Name System (DNS)-based phishing. With a pharming scheme, hackers tamper with a company's hosts files or domain name system so that requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site. The result – users are unaware that the Website where they are entering confidential information is controlled by hackers and is probably not even in the same country as the legitimate Website.

(viii) ***Content-Injection Phishing*** – It describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead or misdirect the user into giving up their confidential information to the hacker. For example, hackers may insert malicious code to log user's credentials or an overlay which can secretly collect information and deliver it to the hacker's phishing server.

(ix) ***Search Engine Phishing*** – It occurs when phishers create Web sites with attractive (often too attractive) sounding offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks. Victims who use these sites to save or make more from interest charges are encouraged to transfer existing accounts and deceived into giving up their details.

Q.51. Write short note on Man-in-the-middle-attack.

(R.G.P.V., Dec. 2010, June 2011)

Ans. Refer to Q.50 (i).

Q.52. Write short note on deceptive phishing.

(R.G.P.V., Dec. 2010, June 2011)

Ans. Refer to Q.50 (v).

Q.53. Explain Man-in-middle, phishing and ransomware attacks.

(R.G.P.V., Dec. 2017)

Ans. **Phishing** – Refer to Q.48.

Man-in-middle – Refer to Q.50 (i).

Ransomware – Ransomware is a type of malware. The developer of ransomware blocks the some important files and then blackmail the owner of files to unblock the files. Wannacry is an example of ransomware which infected NHS computers and immediately spread via its network. Ransomware generally spread within PDF file, word documents and other files which are sent through email or through infected PC.

Q.54. What is phishing ? Explain DNS-based phishing.

(R.G.P.V., Dec. 2014)

Ans. Refer to Q.48 and Q.50 (vii).

Q.55. What you can do to avoid phishing attacks ?

Or

Write about offering phishing prevention techniques.

(R.G.P.V., June 2016)

Ans. The good news is there are things you can do to steer clear of phishing attacks and phishing sites –

(i) ***Be Careful about Responding to e-mails that ask you for Sensitive Information*** – You should be wary of clicking on links in e-mails or responding to emails that are asking for things like account numbers, user names and passwords, or other personal information such as social security numbers. Most legitimate businesses will never ask for this information via e-mail. Google does not.

(ii) ***Go to the Site Yourself, Rather than Clicking on Links in Suspicious e-mails*** – If you receive a communication asking for sensitive information but think it could be legitimate, open a new browser window and go to the organization's Website as you normally would (for instance, by using a bookmark or by typing out the address of the organization's Website). This will improve the chances that you are dealing with the organization's Website rather than with a phisher's Website, and if there's actually something you need to do, there will usually be a notification on the site. Also, if you're not sure about a request you have received, do not be afraid to contact the organization directly to ask. It takes just a few minutes to go to the organization's Website, find an e-mail address or phone number for customer support, and reach out to confirm whether the request is legitimate.

(iii) ***If You are on a Site that's Asking you to Enter Sensitive Information, Check for Signs of anything Suspicious*** – If you are on a site that's asking for sensitive information – no matter how you got there – check for the signs that it's really the official Website for the organization. For example, check the URL to make sure the page is actually part of the organization's website, and not a fraudulent page on a different domain (such as mybankk.com

or g00gle.com.) If you're on a page that should be secured (like one asking you to enter in your credit card information) look for "https" at the beginning of the URL and the padlock icon in the browser. (In Firefox and Internet Explorer 6, the padlock appears in the bottom right-hand corner, while in Internet Explorer 7 the padlock appears on the right-hand side of the address bar.) These signs are not infallible, but they are a good place to start.

(iv) Be Wary of the "Fabulous Offers" and "Fantastic Prizes" that You will Sometimes come Across on the Web – If something seems too good to be true, it probably is, and it could be a phisher trying to steal your information. Whenever you come across an offer online that requires you to share personal or other sensitive information to take advantage of it, be sure to ask lots of questions and check the site asking for your information for signs of anything suspicious.

(v) Use of Browser that has a Phishing Filter – The latest versions of most browsers include phishing filters that can help you spot potential phishing attacks.

Q.56. What are security threats ? ***(R.G.P.V., Nov. 2019)***

Ans. Within the framework of cyber security, the term threat refers to the potential dangers that can harm the files within your systems, operations of your systems or your networks. As the businesses are depending on the digital more heavily each day, the types and scope of cyber security threats constantly change and evolve. There are several major categories of cyber security threats such as Ransom ware, malware, social engineering and phishing.

(i) ***Ransom ware*** is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.

(ii) ***Malware*** is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.

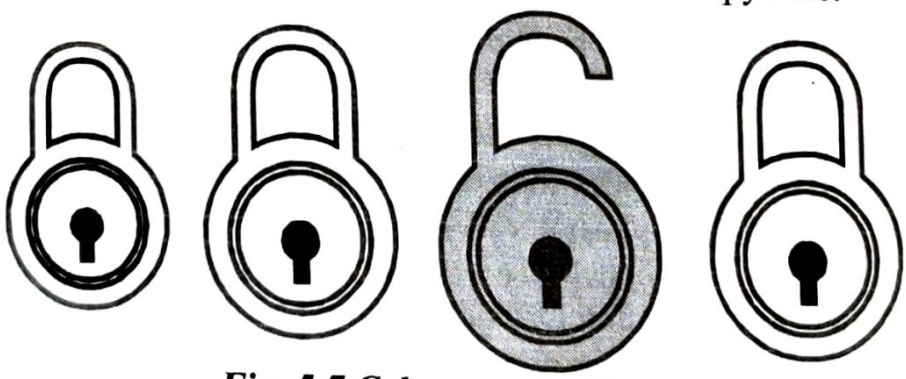


Fig. 5.7 Cybersecurity Threats

(iii) ***Social engineering*** is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

(iv) ***Phishing*** is a form of fraud where fraudulent e-mails are sent that resemble emails from reputable sources; however, the intention of these e-mails is to steal sensitive data, such as credit card or login information.

■■■

RGPV

CS-5005 (2) (CBGS)
B.E. (Fifth Semester) EXAMINATION, Nov. 2018
Choice Based Grading System (CBGS)
CYBER SECURITY

Note – **(i)** Attempt any five questions.
(ii) All questions carry equal marks.

1. **(a)** Define the term cyber crime. Give the classification of cyber crime.
(See Unit-I, Page 4, Q.3)

(b) What can a person do to protect himself/herself from identity theft ?
(See Unit-II, Page 34, Q.24)

2. **(a)** What are the problems may be generate due session hijacking ?

(b) Define the term cyber stalking. How can we tackle this cyber crime ?
(See Unit-I, Page 9, Q.9)

3. **(a)** How can we check the validity of digital evidence ?
(See Unit-IV, Page 85, Q.22)

(b) What is the Salami attack ? How information can be gathered through Salami technique ?
(See Unit-I, Page 11, Q.12)

4. **(a)** Explain the different types of phishing. **(See Unit-V, Page 119, Q.50)**

(b) What is the role of digital signature in digital evidence ?
(See Unit-IV, Page 85, Q.21)

5. **(a)** How DoS and DDoS attacks can be performed ?
(See Unit-V, Page 112, Q.41)

(b) What is IT Act 2000 ? Write the silent features of IT Act 2000.
(See Unit-III, Page 50, Q.2)

6. **(a)** What is computer virus ? How the virus spread ? How to protect against virus ?
(See Unit-V, Page 97, Q.19)

(b) How Trojan horses affect the computer system/network ?
(See Unit-V, Page 103, Q.27)

7. **(a)** What is anonymizers ? How anonymizers work ?
(See Unit-V, Page 88, Q.2)

(b) What is the cyber terrorism ? Discuss in detail.
(See Unit-II, Page 39, Q.28)

8. Write the short notes on –
(a) E-mail spoofing **(See Unit-I, Page 6, Q.5)**
(b) Software piracy **(See Unit-II, Page 19, Q.4)**
(c) Password sniffing **(See Unit-II, Page 31, Q.21)**
(d) Key loggers. **(See Unit-V, Page 89, Q.5)**

RGPV

CS-503 (C) (CBGS)
B. Tech (Fifth Semester)
EXAMINATION, Nov. 2019
Choice Based Grading System (CBGS)
CYBER SECURITY

Note – **(i)** Attempt any five questions.
(ii) All questions carry equal marks.
(iii) All parts of each questions are to be attempted at one place.

1. **(a)** What do you mean by IP spoofing ? **(See Unit-1, Page 6, Q.5)** 7

(b) What is computer virus ? How the virus spread ? 7
(See Unit-V, Page 94, Q.11)

2. **(a)** Discuss the components of digital signature. 7
(See Unit-IV, Page 75, Q.11)

(b) Explain intellectual property right with suitable example. 7
(See Unit-III, Page 64, Q.20)

3. **(a)** How can we check the validity of digital evidence ? 7
(See Unit-IV, Page 85, Q.22)

(b) Define the term cyber stalking. How can we tackle this cyber crime ?
(See Unit-I, Page 9, Q.9) 7

4. **(a)** What do you mean by session hijacking ? **(See Unit-II, Page 46, Q.36)** 7

(b) What are the various challenges of cyber crime ? 7
(See Unit-I, Page 4, Q.2)

5. **(a)** What are security threats ? **(See Unit-V, Page 126, Q.56)** 7

(b) Explain the term phishing in detail. **(See Unit-V, Page 118, Q.48)** 7

6. **(a)** Explain the term copyright act and patent law. 7
(See Unit-III, Page 65, Q.21)

(b) Discuss the concept of intrusion detection system. 7
(See Unit-II, Page 21, Q.9)

7. **(a)** What do you mean by software piracy ? **(See Unit-II, Page 19, Q.4)** 7

(b) Why we need cyber security explain ? **(See Unit-III, Page 52, Q.5)** 7

8. Write down short notes on any three – 14

(a) Backdoor **(See Unit-V, Page 106, Q.31)**
(b) Logic bomb **(See Unit-V, Page 107, Q.32)**
(c) Worm **(See Unit-V, Page 98, Q.20)**
(d) Spyware **(See Unit-V, Page 90, Q.6)**
(e) Firewalls. **(See Unit-V, Page 107, Q.33)**